Global Inspiration
세계속의 경기도

2016. 8. 31. 기준 법령 수록

개인정보보호 법령집

NEXT 경기

경 기 도

목 차

Ⅰ. 법령

1. 개인정보보호법
2. 개인정보보호법 시행령
3. 개인정보보호법 시행규칙

Ⅱ. 예규, 훈령, 고시

1. 표준 개인정보 보호지침[전문]
2. 개인정보의 안전성 확보조치 기준
3. 개인정보 영향평가에 관한 고시
4. 개인정보보호 관리체계 인증 등에 관한 고시
5. 개인정보보호 자율규제단체 지정 등에 관한 규정

Ⅲ. 가이드, 해설서

1. 개인정보의 안전성 확보조치 기준 해설서
2. 홈페이지 개인정보 노출방지 안내서
3. 개인정보 수집제공 동의서 작성 가이드라인
4. 공공기관 개인정보 영향평가 수행 시 참고사항
5. 주민등록번호 수집 금지 제도 가이드라인
6. 개인정보 비식별 조치 가이드라인
7. 개인정보 암호화 조치 안내서
8. 시스템 개발.운영자를 위한 개인정보보호 가이드라인
9. CCTV 설치 · 운영 가이드라인 개정안
10. 개인정보보호 자율점검 가이드라인

Ⅳ. 경기도 조례, 매뉴얼

1. 경기도 개인정보 보호 조례
2. 경기도 개인영상정보 보호 및 영상정보처리기기 설치 운영 조례
3. 경기도 개인정보 목적 외 이용제공 절차서
4. 경기도 개인정보 유출 대응 매뉴얼

Ⅴ. 기타

1. 개인정보처리방침 작성예시
2. 개인정보처리 위탁계약서 표준 양식
3. 개인정보 유출 시 필수 조치요령
4. 분야별 주민등록번호 처리기준 상담사례집

개인정보보호법/시행령/시행규칙

개인정보 보호법

[시행 2016.7.25.] [법률 제13423호, 2015.7.24., 일부개정]
행정자치부 (개인정보보호정책과) 02 - 2100 - 4105

제1장 총칙

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. <개정 2014.3.24.>

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24.>

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. "공공기관"이란 다음 각 목의 기관을 말한다.
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
   나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리

2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

제5조(국가 등의 책무) ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.

② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.

③ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.

④ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 이 법의 목적에 부합되도록 하여야 한다.

제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. <개정 2014.3.24.>

제2장 개인정보 보호정책의 수립 등

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다.

② 보호위원회는 위원장 1명, 상임위원 1명을 포함한 15명 이내의 위원으로 구성하되, 상임위원은 정무직 공무원으로 임명한다.

③ 위원장은 위원 중에서 공무원이 아닌 사람으로 대통령이 위촉한다.

④ 위원은 다음 각 호의 어느 하나에 해당하는 사람을 대통령이 임명하거나 위촉한다. 이 경우 위원 중 5명은 국회가 선출하는 자를, 5명은 대법원장이 지명하는 자를 각각 임명하거나 위촉한다.

1. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람
3. 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람

⑤ 위원장과 위원의 임기는 3년으로 하되, 1차에 한하여 연임할 수 있다.

⑥ 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

⑦ 보호위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회의 사무를 지원하기 위하여 보호위원회에 사무국을 둔다.

⑨ 제1항부터 제8항까지에서 규정한 사항 외에 보호위원회의 조직과 운영에 필요한 사항은 대통령령으로 정한다.

제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. <개정 2015.7.24.>

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
1의2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획
2. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
4. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
5. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
6. 제33조제3항에 따른 영향평가 결과에 관한 사항

7. 제61조제1항에 따른 의견제시에 관한 사항
8. 제64조제4항에 따른 조치의 권고에 관한 사항
9. 제66조에 따른 처리 결과의 공표에 관한 사항
10. 제67조제1항에 따른 연차보고서의 작성·제출에 관한 사항
11. 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
12. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항

② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다.<개정 2015.7.24.>

1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취
2. 관계 기관 등에 대한 자료제출이나 사실조회 요구

③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 응하여야 한다.<신설 2015.7.24.>

④ 보호위원회는 제1항제2호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다.<신설 2015.7.24.>

⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.<신설 2015.7.24.>

제8조의2(개인정보 침해요인 평가) ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.

② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다.

③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.7.24.]

제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013.3.23., 2014.11.19., 2015.7.24.>

② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.

제10조(시행계획) ① 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.

② 시행계획의 수립·시행에 필요한 사항은 대통령령으로 정한다.

제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. <개정 2013.3.23., 2014.11.19., 2015.7.24.>

② 행정자치부장관은 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를

실시할 수 있다.<신설 2015.7.24.>

③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다.<개정 2015.7.24.>

④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.<개정 2015.7.24.>

⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다.<개정 2015.7.24.>

제12조(개인정보 보호지침) ① 행정자치부장관은 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 "표준지침"이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

제13조(자율규제의 촉진 및 지원) 행정자치부장관은 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다. <개정 2013.3.23., 2014.11.19.>

1. 개인정보 보호에 관한 교육·홍보
2. 개인정보 보호와 관련된 기관·단체의 육성 및 지원
3. 개인정보 보호 인증마크의 도입·시행 지원
4. 개인정보처리자의 자율적인 규약의 제정·시행 지원
5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

제14조(국제협력) ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.

② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집ㆍ이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.<신설 2013.8.6.>

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.<개정 2013.8.6.>

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호ㆍ제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

제18조(개인정보의 목적 외 이용ㆍ제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의ㆍ의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정자치부령으로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.<개정 2013.3.23., 2014.11.19.>

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

[제목개정 2013.8.6.]

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 제1항은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.

1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 제1항에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조제1항제1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.<신설 2016.3.29.>

③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기·방법 및 절차 등 필요한 사항은 대통령령으로 정한다.<신설 2016.3.29.>

④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.<개정 2016.3.29.>

1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

[시행일 : 2016.9.30.] 제20조

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

② 개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

② 개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1항제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.<개정 2016.3.29.>

③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는

아니 된다.

⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

[시행일 : 2016.9.30.] 제22조

제2절 개인정보의 처리 제한

제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

제23조(민감정보의 처리 제한) ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29.>

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.<신설 2016.3.29.>

[시행일 : 2016.9.30.] 제23조

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제<2013.8.6.>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24.>

④ 삭제<2013.8.6.>

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제<2013.8.6.>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24.>

④ 행정자치부장관은 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.<신설 2016.3.29.>

⑤ 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.<신설 2016.3.29.>

[시행일 : 2016.9.30.] 제24조

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.<신설 2014.3.24., 2015.7.24.>

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.<개정 2014.3.24.>

④ 안전행정부장관은 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.<개정 2014.3.24.>

[본조신설 2013.8.6.]

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. <개정 2016.3.29.>

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.<신설 2014.3.24., 2015.7.24.>

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.<개정 2014.3.24.>

④ 안전행정부장관은 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.<개정 2014.3.24.>

[본조신설 2013.8.6.]
[시행일 : 2017.3.30.] 제24조의2제1항제1호

제25조(영상정보처리기기의 설치 · 운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24.>

⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

제25조(영상정보처리기기의 설치 · 운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만,

「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.<개정 2016.3.29.>

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24.>

⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

[시행일 : 2016.9.30.] 제25조

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.<개정 2015.7.24.>

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

제27조(영업양도 등에 따른 개인정보의 이전 제한) ① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.
③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 "개인정보취급자"라 한다)에 대하여 적절한 관리·감독을 행하여야 한다.
② 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

제4장 개인정보의 안전한 관리

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24.>

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.
1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항
6. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.
④ 행정자치부장관은 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.<개정 2013.3.23., 2014.11.19.>

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29.>
1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)

8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.

④ 행정자치부장관은 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.<개정 2013.3.23., 2014.11.19.>

[시행일 : 2016.9.30.] 제30조

제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

③ 개인정보 보호책임자는 제2항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

⑤ 개인정보처리자는 개인정보 보호책임자가 제2항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다.

⑥ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 행정자치부장관에게 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다. <개정 2013.3.23., 2014.11.19.>

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령으로 정하는 사항

② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

③ 행정자치부장관은 필요하면 제1항에 따른 개인정보파일의 등록사항과 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.<개정 2013.3.23., 2014.11.19.>
④ 행정자치부장관은 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다. <개정 2013.3.23., 2014.11.19.>
⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법, 범위 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.
⑥ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

제32조의2(개인정보 보호 인증) ① 행정자치부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.
② 제1항에 따른 인증의 유효기간은 3년으로 한다.
③ 행정자치부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다.
1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우
④ 행정자치부장관은 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다.
⑤ 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다.
⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.
⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.
⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.
[본조신설 2015.7.24.]

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정자치부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다. <개정 2013.3.23., 2014.11.19.>
② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.
1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항
③ 행정자치부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.<개정 2013.3.23., 2014.11.19.>
④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.
⑤ 행정자치부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.<개정 2013.3.23., 2014.11.19.>
⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.
⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.
1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.<개정 2013.3.23., 2014.11.19.>
④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제34조의2(과징금의 부과 등) ① 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다. <개정 2014.11.19., 2015.7.24.>
② 행정자치부장관은 제1항에 따른 과징금을 부과하는 경우에는 다음 각 호의 사항을 고려하여야 한다.<개정 2014.11.19., 2015.7.24.>
1. 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도
2. 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도
3. 피해확산 방지를 위한 후속조치 이행 여부

③ 행정자치부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.<개정 2014.11.19.>
④ 행정자치부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 제2항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.<개정 2014.11.19.>
⑤ 과징금의 부과·징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다.
[본조신설 2013.8.6.]

제5장 정보주체의 권리 보장

제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.
② 제1항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 행정자치부장관을 통하여 열람을 요구할 수 있다.<개정 2013.3.23., 2014.11.19.>

③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.

④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
   가. 조세의 부과·징수 또는 환급에 관한 업무
   나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
   다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
   라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
   마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

⑤ 제1항부터 제4항까지의 규정에 따른 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.

⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.

② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.
④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.
⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.
③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
② 삭제<2015.7.24.>
③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.<신설 2015.7.24.>
④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.<신설 2015.7.24.>
1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.
③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015.7.24.]

제6장 개인정보 분쟁조정위원회

제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.

② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.<개정 2015.7.24.>

③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.<개정 2013.3.23., 2014.11.19., 2015.7.24.>

1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.<개정 2013.3.23., 2014.11.19., 2015.7.24.>

⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.<개정 2015.7.24.>

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.<개정 2015.7.24.>

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

제41조(위원의 신분보장) 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

제42조(위원의 제척·기피·회피) ① 분쟁조정위원회의 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 제43조제1항에 따라 분쟁조정위원회에 신청된 분쟁조정사건(이하 이 조에서 "사건"이라 한다)의 심의·의결에서 제척(除斥)된다.

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우
3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 분쟁조정위원회의 의결을 거치지 아니하고 결정한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결에서 회피할 수 있다.

제43조(조정의 신청 등) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다.

② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.
③ 공공기관이 제2항에 따른 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다.

제44조(처리기간) ① 분쟁조정위원회는 제43조제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.
② 분쟁조정위원회는 제1항 단서에 따라 처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

제45조(자료의 요청 등) ① 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 해당 분쟁의 조정을 위하여 필요한 자료를 분쟁당사자에게 요청할 수 있다. 이 경우 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.
② 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다.

제46조(조정 전 합의 권고) 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

제47조(분쟁의 조정) ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.
1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치
② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.
③ 제1항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 거부한 것으로 본다.
④ 당사자가 조정내용을 수락한 경우 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인하여야 한다.
⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

제48조(조정의 거부 및 중지) ① 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.
② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다.

제49조(집단분쟁조정) ① 국가 및 지방자치단체, 개인정보 보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 "집단분쟁조정"이라 한다)을 의뢰 또는 신청할 수 있다.
② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.
③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.
④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.

⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.
⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.
⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.
⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제50조(조정절차 등) ① 제43조부터 제49조까지의 규정에서 정한 것 외에 분쟁의 조정방법, 조정절차 및 조정업무의 처리 등에 필요한 사항은 대통령령으로 정한다.
② 분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항에 대하여는 「민사조정법」을 준용한다.

제7장 개인정보 단체소송

제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 "단체소송"이라 한다)을 제기할 수 있다.
1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것
   나. 단체의 정회원수가 1천명 이상일 것
   다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
   나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
   다. 단체의 상시 구성원수가 5천명 이상일 것
   라. 중앙행정기관에 등록되어 있을 것

제52조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.
② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제53조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

제54조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.
1. 원고 및 그 소송대리인
2. 피고
3. 정보주체의 침해된 권리의 내용
② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.
1. 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류

제55조(소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.

1. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
2. 제54조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것

② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

제56조(확정판결의 효력) 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제51조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우
2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

제57조(「민사소송법」의 적용 등) ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.

② 제55조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다.

③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

제8장 보칙

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보

② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.

③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

1. 제8조에 따른 보호위원회의 업무

2. 제33조에 따른 영향평가 업무
3. 제40조에 따른 분쟁조정위원회의 분쟁조정 업무

제61조(의견제시 및 개선권고) ① 행정자치부장관은 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 보호위원회의 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 행정자치부장관은 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 행정자치부장관에게 알려야 한다.<개정 2013.3.23., 2014.11.19.>

③ 관계 중앙행정기관의 장은 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.

④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 행정자치부장관에게 그 침해 사실을 신고할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 행정자치부장관은 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 "신고센터"라 한다)를 설치·운영하여야 한다.<개정 2013.3.23., 2014.11.19.>

③ 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 사실의 조사·확인 및 관계자의 의견 청취
3. 제1호 및 제2호에 따른 업무에 딸린 업무

④ 행정자치부장관은 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.<개정 2013.3.23., 2014.11.19.>

제63조(자료제출 요구 및 검사) ① 행정자치부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다. <개정 2013.3.23., 2014.11.19.>

1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 행정자치부장관은 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.<개정 2013.3.23., 2014.11.19., 2015.7.24.>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에게 제1항에 따른 자료제출을 요구하거나 개인정보처리자 및 해당 법 위반사실과 관련한 관계인에 대하여 제2항에 따른 검사를 할 수 있다.<개정 2015.7.24.>

④ 보호위원회는 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우에는 행정자치부장관 또는 관계 중앙행정기관의 장에게 제1항 각 호 외의 부분 또는 제3항에 따른 조치를 하도록 요구할 수 있다. 이 경우 그 요구를 받은 행정자치부장관 또는 관계 중앙행정기관의 장은 특별한 사정이 없으면 이에 응하여야 한다.<신설 2015.7.24.>

⑤ 행정자치부장관과 관계 중앙행정기관의 장은 제1항 및 제2항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다.<개정 2013.3.23.,

2014.11.19., 2015.7.24.>

⑥ 행정자치부장관과 관계 중앙행정기관의 장은 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다. <개정 2013.3.23., 2014.11.19., 2015.7.24.>

⑦ 행정자치부장관은 개인정보 침해사고의 예방과 효과적인 대응을 위하여 관계 중앙행정기관의 장과 합동으로 개인정보 보호실태를 점검할 수 있다.<신설 2015.7.24.>

제64조(시정조치 등) ① 행정자치부장관은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다. <개정 2013.3.23., 2014.11.19.>

1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치

② 관계 중앙행정기관의 장은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 소관 법률에 따라 개인정보처리자에 대하여 제1항 각 호에 해당하는 조치를 명할 수 있다.

③ 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.

④ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.

제65조(고발 및 징계권고) ① 행정자치부장관은 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 행정자치부장관은 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 행정자치부장관에게 통보하여야 한다.<개정 2013.3.23., 2013.8.6., 2014.11.19.>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제66조(결과의 공표) ① 행정자치부장관은 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과의 내용 및 결과에 대하여 보호위원회의 심의·의결을 거쳐 공표할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 관계 중앙행정기관의 장은 소관 법률에 따라 제1항에 따른 공표를 할 수 있다.

③ 제1항 및 제2항에 따른 공표의 방법, 기준 및 절차 등은 대통령령으로 정한다.

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다.

1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보 처리에 관한 실태조사 등의 결과
3. 개인정보 보호시책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고하여야 할 사항

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다.<개정 2016.3.29.>

1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보 처리에 관한 실태조사 등의 결과
3. 개인정보 보호시책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙의 제정·개정 현황
6. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고하여야 할 사항

[시행일 : 2017.3.30.] 제67조제2항제5호

제68조(권한의 위임·위탁) ① 이 법에 따른 행정자치부장관 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다. <개정 2013.3.23., 2014.11.19.>

② 제1항에 따라 행정자치부장관 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 행정자치부장관 또는 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013.3.23., 2014.11.19.>

③ 행정자치부장관은 제1항에 따른 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다.<개정 2013.3.23., 2014.11.19.>

제69조(벌칙 적용 시의 공무원 의제) 행정자치부장관 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 「형법」 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다. <개정 2013.3.23., 2014.11.19.>

제9장 벌칙

제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <개정 2015.7.24.>

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

3. 제23조를 위반하여 민감정보를 처리한 자
4. 제24조제1항을 위반하여 고유식별정보를 처리한 자
5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.29.>

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제23조제1항을 위반하여 민감정보를 처리한 자
4. 제24조제1항을 위반하여 고유식별정보를 처리한 자
5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자

[시행일 : 2016.9.30.] 제71조

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
2. 제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2015.7.24.>

1. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자
2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2015.7.24., 2016.3.29.>

1. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자
2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

[시행일 : 2016.9.30.] 제73조

제74조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하

지 아니한 경우에는 그러하지 아니하다.

② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

제74조의2(몰수·추징 등) 제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

[본조신설 2015.7.24.]

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제15조제1항을 위반하여 개인정보를 수집한 자
2. 제22조제5항을 위반하여 법정대리인의 동의를 받지 아니한 자
3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.<개정 2013.8.6., 2014.3.24., 2015.7.24.>

1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
2. 제16조제3항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 자
3. 제20조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
4. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 자

4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자

4의3. 제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자

5. 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
6. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자

7의2. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자

8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자
10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자
11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자
13. 제64조제1항에 따른 시정명령에 따르지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자
2. 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 자
3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자
4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자
5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자
6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자
7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자
8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자

10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자
11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자

④ 제1항부터 제3항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 행정자치부장관과 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다.<개정 2013.3.23., 2014.11.19.>

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제15조제1항을 위반하여 개인정보를 수집한 자
2. 제22조제5항을 위반하여 법정대리인의 동의를 받지 아니한 자
3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.<개정 2013.8.6., 2014.3.24., 2015.7.24., 2016.3.29.>

1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
2. 제16조제3항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 자
3. 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
4. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 자

4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자

4의3. 제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자

5. 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
6. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자

7의2. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자

8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자
10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자
11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자
13. 제64조제1항에 따른 시정명령에 따르지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자
2. 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 자
3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자
4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자
5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자
6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자
7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자
8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자
11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자

④ 제1항부터 제3항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 행정자치부장관과 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다.<개정 2013.3.23., 2014.11.19.>

[시행일 : 2016.9.30.] 제75조

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.

[본조신설 2013.8.6.]

부칙 <제10465호,2011.3.29.>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제24조제2항 및 제75조제2항제5호는 공포 후 1년이 경과한 날부터 시행한다.

제2조(다른 법률의 폐지) 공공기관의 개인정보보호에 관한 법률은 폐지한다.

제3조(개인정보분쟁조정위원회에 관한 경과조치) 이 법 시행 당시 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 개인정보분쟁조정위원회의 행위나 개인정보분쟁조정위원회에 대한 행위는 그에 해당하는 이 법에 따른 개인정보 분쟁조정위원회의 행위나 개인정보 분쟁조정위원회에 대한 행위로 본다.

제4조(처리 중인 개인정보에 관한 경과조치) 이 법 시행 전에 다른 법령에 따라 적법하게 처리된 개인정보는 이 법에 따라 처리된 것으로 본다.

제5조(벌칙의 적용에 관한 경과조치) ① 이 법 시행 전에 종전의 「공공기관의 개인정보보호에 관한 법률」을 위반한 행위에 대하여 벌칙을 적용할 때에는 종전의 「공공기관의 개인정보보호에 관한 법률」에 따른다.

② 이 법 시행 전에 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반한 행위에 대하여 벌칙을 적용할 때에는 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른다.

제6조(다른 법률의 개정) ① 6·25 전사자유해의 발굴 등에 관한 법률 일부를 다음과 같이 개정한다.

제14조제1항제2호 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

② 공직자윤리법 일부를 다음과 같이 개정한다.

제6조제6항 및 제9항 중 "「공공기관의 개인정보보호에 관한 법률」 제10조"를 각각 "「개인정보 보호법」 제18조"로 한다.

③ 국가공무원법 일부를 다음과 같이 개정한다.

제19조의3제3항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제1호"를 "「개인정보 보호법」 제2조제6호"로 하고, 같은 조 제4항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

④ 발명진흥법 일부를 다음과 같이 개정한다.

제20조의2제1항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑤ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제23조제2항제2호를 다음과 같이 한다.

2. 「개인정보 보호법」

⑥ 아동복지법 일부를 다음과 같이 개정한다.

제9조의2제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑦ 법률 제10333호 암관리법 전부개정법률 일부를 다음과 같이 개정한다.

제14조제1항 후단 중 "「공공기관의 개인정보보호에 관한 법률」 제3조제2항"을 "「개인정보 보호법」 제58조제1항"으로 한다.

제49조 중 "「공공기관의 개인정보보호에 관한 법률」 제10조제3항"을 "「개인정보 보호법」 제18조제2항"으로 한다.

⑧ 장애인차별금지 및 권리구제 등에 관한 법률 일부를 다음과 같이 개정한다.

제3조제8호다목 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

제22조제2항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑨ 전자서명법 일부를 다음과 같이 개정한다.

제24조제2항을 삭제한다.

⑩ 전자정부법 일부를 다음과 같이 개정한다.

제21조제2항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

제39조제4항 중 "「공공기관의 개인정보보호에 관한 법률」 제5조"를 "「개인정보 보호법」 제32조"로, "같은 법 제20조제1항에 따른 공공기관개인정보보호심의위원회의 심의를 거쳐"를 "「개인정보 보호법」 제7조에 따른 개인정보 보호위원회의 심의·의결을 거쳐"로 한다.

제42조제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제8호"를 "「개인정보 보호법」 제2조제3호"로, "「공공기관의 개인정보보호에 관한 법률」 제10조제3항제1호 및 같은 조 제5항은"을 "「개인정보 보호법」 제18조제2항제1호 및 제19조제1호는"으로 한다.

⑪ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부를 다음과 같이 개정한다.

제4장제4절(제33조, 제33조의2, 제34조부터 제40조까지), 제66조제1호 및 제67조를 각각 삭제한다.

제4조제1항·제3항, 제64조의2제3항 후단, 제65조제1항 및 제69조 중 "행정안전부장관, 지식경제부장관 또는 방송통신위원회"를 각각 "지식경제부장관 또는 방송통신위원회"로 한다.

제64조제1항 각 호 외의 부분·제3항·제4항 전단·제5항 전단·제6항·제9항·제10항, 제64조의2제1항·제2항·제3항 각 호 외의 부분 전단, 제65조제3항, 제76조제1항제12호 및 제4항부터 제6항까지 중 "행정안전부장관 또는 방송통신위원회"를 각각 "방송통신위원회"로 한다.

⑫ 채권의 공정한 추심에 관한 법률 일부를 다음과 같이 개정한다.

제2조제5호 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

⑬ 출입국관리법 일부를 다음과 같이 개정한다.

제12조의2제6항 및 제38조제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 각각 "「개인정보 보호법」"으로 한다.

⑭ 한국장학재단 설립 등에 관한 법률 일부를 다음과 같이 개정한다.

제50조제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

제7조(다른 법령과의 관계) 이 법 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률」 또는 그 규정을 인용하고 있는 경우 이 법 중 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 법 또는 이 법의 해당 규정을 인용한 것으로 본다.

부칙 <제11690호,2013.3.23.>

제1조(시행일) ① 이 법은 공포한 날부터 시행한다.

②생략

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <149>까지 생략

<150> 개인정보 보호법 일부를 다음과 같이 개정한다.

제9조제1항, 제11조제1항, 제12조제1항, 제13조 각 호 외의 부분, 제24조제4항, 제30조제4항, 제32조제1항 각 호 외의 부분 전단, 같은 조 제3항ㆍ제4항, 제33조제1항 전단ㆍ후단, 같은 조 제3항ㆍ제5항, 제34조제3항 전단ㆍ후단, 제35조제2항, 제40조제3항 각 호 외의 부분, 같은 조 제4항ㆍ제8항, 제61조제1항, 같은 조 제2항 전단ㆍ후단, 제62조제1항, 같은 조 제2항 전단, 같은 조 제4항, 제63조제1항 각 호 외의 부분, 같은 조 제2항 전단, 같은 조 제4항ㆍ제5항, 제64조제1항 각 호 외의 부분, 제65조제1항, 같은 조 제2항 전단ㆍ후단, 제66조제1항, 제68조제1항부터 제3항까지, 제69조 및 제75조제4항 전단 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

제18조제4항 중 "행정안전부령"을 "안전행정부령"으로 한다.

<151>부터 <710>까지 생략

제7조 생략

부칙 <제11990호,2013.8.6.>

제1조(시행일) 이 법은 공포 후 1년이 경과한 날부터 시행한다.

제2조(주민등록번호 처리 제한에 관한 경과조치) ① 이 법 시행 당시 주민등록번호를 처리하고 있는 개인정보처리자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제24조의2제1항 각 호의 개정규정의 어느 하나에 해당하는 경우는 제외한다.

② 제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제24조의2제1항의 개정규정을 위반한 것으로 본다.

부칙 <제12504호,2014.3.24.>

이 법은 공포한 날부터 시행한다. 다만, 법률 제11990호 개인정보 보호법 일부개정법률 제24조의2 및 제75조제2항제5호의 개정규정은 2016년 1월 1일부터 시행한다.

부칙 <제12844호,2014.11.19.>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 법률 중 이 법 시행 전에 공포되었으나 시행일이 도래하지 아니한 법률을 개정한 부분은 각각 해당 법률의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <55>까지 생략

<56> 개인정보 보호법 일부를 다음과 같이 개정한다.

제9조제1항, 제11조제1항, 제12조제1항, 제13조 각 호 외의 부분, 제24조의2제1항제3호, 제30조제4항, 제32조제1항 각 호 외의 부분 전단, 같은 조 제3항·제4항, 제33조제1항 전단·후단, 같은 조 제3항·제5항, 제34조제3항 전단·후단, 제34조의2제1항 본문, 같은 조 제2항 각 호 외의 부분, 같은 조 제3항 전단, 같은 조 제4항, 제35조제2항, 제40조제3항 각 호 외의 부분, 같은 조 제4항·제8항, 제61조제1항, 같은 조 제2항 전단·후단, 제62조제1항, 같은 조 제2항 전단, 같은 조 제4항, 제63조제1항 각 호 외의 부분, 같은 조 제2항 전단, 같은 조 제4항·제5항, 제64조제1항 각 호 외의 부분, 제65조제1항, 같은 조 제2항 전단·후단, 제66조제1항, 제68조제1항부터 제3항까지, 제69조 및 제75조제4항 전단 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

제18조제4항 중 "안전행정부령"을 "행정자치부령"으로 한다.

<57>부터 <258>까지 생략

제7조 생략

부칙 <제13423호,2015.7.24.>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 제8조제1항, 제8조의2, 제9조, 제11조제1항, 제32조의2, 제39조제3항·제4항, 제39조의2, 제40조, 제75조제2항제7호의2의 개정규정은 공포 후 1년이 경과한 날부터, 법률 제12504호 개인정보 보호법 일부개정법률 제24조의2제2항 전단 및 제75조제2항제4호의3의 개정규정은 2016년 1월 1일부터 각각 시행한다.

제2조(손해배상에 관한 적용례) 제39조제3항·제4항 및 제39조의2의 개정규정은 이 법 시행 후에 분실·도난·유출·위조·변조 또는 훼손된 개인정보에 관한 손해배상 청구분부터 적용한다.

제3조(개인정보 보호 인증에 관한 경과조치) 이 법 시행 전에 행정자치부장관으로부터 개인정보 보호 인증을 받은 자는 제32조의2의 개정규정에 따른 개인정보 보호 인증을 받은 것으로 본다.

제4조(개인정보 인증 심사원 자격에 관한 경과조치) 이 법 시행 전에 개인정보 보호 인증 심사원의 자격을 취득한 자는 이 법에 따른 개인정보 보호 인증 심사원의 자격을 취득한 것으로 본다.

제5조(개인정보 분쟁조정위원회 위원의 임기에 관한 경과조치) 이 법 시행 전에 행정자치부장관이 임명하거나 위촉한 분쟁조정위원회 위원은 제40조의 개정규정에 따른 보호위원회가 위촉한 분쟁조정위원회 위원으로 본다.

제6조(벌칙 등에 관한 경과조치) 이 법 시행 전의 위반행위에 대하여 벌칙 또는 과태료를 적용할 때에는 종전의 규정에 따른다.

개인정보 보호법 시행령

[시행 2016.7.25.] [대통령령 제27370호, 2016.7.22., 일부개정]
행정자치부 (개인정보보호정책과) 02 - 2100 - 4105

제1장 총칙

제1조(목적) 이 영은 「개인정보 보호법」에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관의 범위) 「개인정보 보호법」(이하 "법"이라 한다) 제2조제6호나목에서 "대통령령으로 정하는 기관"이란 다음 각 호의 기관을 말한다.

1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
3. 「지방공기업법」에 따른 지방공사와 지방공단
4. 특별법에 따라 설립된 특수법인
5. 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교

제3조(영상정보처리기기의 범위) 법 제2조제7호에서 "대통령령으로 정하는 장치"란 다음 각 호의 장치를 말한다.

1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치
   가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
   나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라: 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

제2장 개인정보 보호위원회

제4조(위원의 제척·기피·회피) ① 법 제7조제2항에 따른 개인정보 보호위원회(이하 "보호위원회"라 한다)의 위원은 다음 각 호의 어느 하나에 해당하는 사항에 대한 심의·의결에 관여하지 못한다.

1. 위원 또는 위원의 배우자, 4촌 이내의 혈족, 2촌 이내의 인척인 사람이나 그 사람이 속한 기관·단체와 이해관계가 있는 사항
2. 위원이 증언, 진술 또는 감정(鑑定)을 하거나 대리인으로 관여한 사항
3. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 사항

② 보호위원회가 심의·의결하는 사항과 직접적인 이해관계가 있는 자는 제1항에 따른 제척 사유가 있거나 심의·의결의 공정을 기대하기 어려운 사유가 있는 위원에 대해서는 그 사유를 밝혀 보호위원회에 그 위원의 기피를 신청할 수 있다. 이 경우 위원장이 기피 여부를 결정한다.

③ 위원은 제1항 또는 제2항에 해당하는 경우에는 스스로 심의·의결을 회피할 수 있다.

제5조(전문위원회) ① 보호위원회는 법 제8조제1항에 따른 심의·의결 사항에 대하여 사전에 전문적으로 검토하기 위하여 보호위원회에 분야별 전문위원회(이하 "전문위원회"라 한다)를 둘 수 있다.

② 제1항에 따라 전문위원회를 두는 경우 각 전문위원회는 위원장 1명을 포함한 10명 이내의 위원으로 구성하되, 전문위원회 위원은 다음 각 호의 사람 중에서 보호위원회의 동의를 받아 보호위원회 위원장이 임명하거나 위촉하고, 전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명한다.<개정 2016.7.22.>

1. 보호위원회 위원
2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원

3. 개인정보 보호에 관한 전문지식과 경험이 풍부한 사람
4. 개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람

③ 전문위원회의 회의는 재적위원 과반수의 출석으로 개의(開議)하고, 출석위원 과반수의 찬성으로 의결한다.

제6조(의사의 공개) 보호위원회의 의사(議事)는 공개한다. 다만, 보호위원회 위원장이 필요하다고 인정하는 경우에는 공개하지 아니할 수 있다.

제7조(공무원 등의 파견) 보호위원회는 그 업무 수행을 위하여 필요하다고 인정하는 경우에는 공공기관에 그 소속 공무원 또는 임직원의 파견을 요청할 수 있다.

제8조(조직 및 정원 등) 이 영에서 규정한 사항 외에 보호위원회의 조직 및 정원 등에 관하여 필요한 사항은 따로 대통령령으로 정한다.

제9조(출석수당 등) 보호위원회 또는 전문위원회의 회의에 출석한 위원, 법 제8조제2항에 따라 보호위원회에 출석한 사람 및 전문위원회에 출석한 사람에게는 예산의 범위에서 수당·여비, 그 밖에 필요한 경비를 지급할 수 있다. 다만, 공무원이 그 소관 업무와 직접 관련되어 출석하는 경우에는 그러하지 아니하다.

제9조의2(정책·제도·법령 개선 권고의 절차 등) ① 보호위원회는 법 제8조제4항에 따라 관계 기관에 정책·제도 및 법령의 개선을 권고하는 경우에는 그 내용과 사유 등을 함께 통보하여야 한다.

② 보호위원회는 법 제8조제5항에 따른 권고내용의 이행여부를 점검하기 위하여 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청할 수 있다.

[본조신설 2016.7.22.]

제9조의3(개인정보 침해요인 평가 절차 등) ① 중앙행정기관의 장은 법 제8조의2제1항에 따라 개인정보 침해요인 평가(이하 "침해요인 평가"라 한다)를 요청하는 경우 다음 각 호의 사항을 포함하는 개인정보 침해요인 평가 요청서(전자문서를 포함한다)를 보호위원회에 제출하여야 한다.

1. 법령(법령안을 포함한다)을 통하여 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용
2. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 제2항 각 호의 사항에 대한 개인정보 침해요인 자체 분석
3. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 개인정보 보호 대책

② 보호위원회는 제1항에 따른 요청서를 받은 경우에는 다음 각 호의 사항을 고려하여 침해요인 평가를 하고, 그 결과를 해당 중앙행정기관의 장에게 통보하여야 한다.

1. 개인정보 처리의 필요성
2. 개인정보 주체의 권리보장의 적정성
3. 개인정보 관리의 안전성
4. 그 밖에 침해요인 평가에 필요한 사항

③ 중앙행정기관의 장은 법 제8조의2제2항에 따른 권고를 받은 경우에는 그 내용을 해당 법령안에 반영하는 등 권고내용을 이행하도록 노력하여야 한다. 다만, 보호위원회의 권고대로 이행하기 곤란한 경우에는 그 사유를 보호위원회에 통보하여야 한다.

④ 보호위원회는 침해요인 평가를 하는 경우에는 침해요인 평가에 필요한 자료 등을 해당 중앙행정기관의 장에게 요청할 수 있다.

⑤ 보호위원회는 침해요인 평가의 세부기준 및 방법 등 침해요인 평가에 필요한 지침을 수립하여 중앙행정기관의 장에게 통보할 수 있다.

⑥ 보호위원회는 침해요인 평가를 실시하기 위하여 필요하면 관계 전문가에게 자문 등을 할 수 있다.

[본조신설 2016.7.22.]

제10조(보호위원회 등의 운영 세칙) 법과 이 영에서 규정한 사항 외에 보호위원회 및 전문위원회의 구성 및 운영 등에 필요한 사항은 보호위원회의 의결을 거쳐 보호위원회의 규칙으로 정한다.

제3장 기본계획 및 시행계획의 수립절차

제11조(기본계획의 수립절차 등) ① 보호위원회는 3년마다 법 제9조에 따른 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 그 3년이 시작되는 해의 전전년도 12월 31일까지 수립하여야 한다. <개정 2013.3.23., 2014.11.19., 2016.7.22.>

② 보호위원회는 제1항에 따라 기본계획을 작성하는 경우에는 관계 중앙행정기관의 장으로부터 개인정보 보호 관련 중장기 계획과 시책 등을 반영한 부문별 계획을 제출받아 기본계획에 반영할 수 있다. 이 경우 보호위원회는 기본계획의 목표, 추진방향 및 부문별 계획의 작성 지침 등에 관하여 관계 중앙행정기관의 장과 협의하여야 한다.<개정 2013.3.23., 2014.11.19., 2016.7.22.>

③ 보호위원회는 기본계획이 확정되면 지체 없이 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013.3.23., 2014.11.19., 2016.7.22.>

제12조(시행계획의 수립절차 등) ① 보호위원회는 매년 12월 31일까지 다음다음 해 시행계획의 작성방법 등에 관한 지침을 마련하여 관계 중앙행정기관의 장에게 통보하여야 한다. <개정 2013.3.23., 2014.11.19., 2016.7.22.>

② 관계 중앙행정기관의 장은 제1항의 지침에 따라 기본계획 중 다음 해에 시행할 소관 분야의 시행계획을 작성하여 매년 2월 말일까지 보호위원회에 제출하여야 한다.

③ 보호위원회는 제2항에 따라 제출된 시행계획을 그 해 4월 30일까지 심의·의결하여야 한다.

제13조(자료제출 요구 등의 범위와 방법) ① 보호위원회는 법 제11조제1항에 따라 개인정보처리자에게 다음 각 호의 사항에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. <개정 2013.3.23., 2014.11.19., 2016.7.22.>

1. 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 영상정보처리기기의 설치·운영에 관한 사항
2. 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항
3. 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항
4. 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항
5. 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항

② 보호위원회는 제1항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.<개정 2013.3.23., 2014.11.19., 2016.7.22.>

③ 법 제11조제3항에 따라 중앙행정기관의 장이 소관 분야의 개인정보처리자에게 자료의 제출 등을 요구하는 경우에는 제1항과 제2항을 준용한다. 이 경우 "보호위원회"는 "중앙행정기관의 장"으로, "법 제11조제1항"은 "법 제11조제3항"으로 본다.<개정 2013.3.23., 2014.11.19., 2016.7.22.>

제14조(자율규제의 촉진 및 지원) 행정자치부장관은 법 제13조제2호에 따라 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하기 위하여 예산의 범위에서 개인정보 보호와 관련된 기관 또는 단체에 필요한 지원을 할 수 있다. <개정 2013.3.23., 2014.11.19.>

제4장 개인정보의 처리

제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항 각 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 행정자치부령으로 정하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다. <개정 2013.3.23., 2014.11.19.>

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 법 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

제16조(개인정보의 파기방법) ①개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다. <개정 2014.8.6.>

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.<신설 2014.8.6., 2014.11.19.>

제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

② 개인정보처리자가 정보주체로부터 법 제18조제2항제1호 및 제22조제3항에 따른 동의를 받거나 법 제22조제2항에 따라 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 선택적으로 동의할 수 있는 사항 외의 사항과 구분하여 표시하여야 한다. <신설 2015.12.30.>

③ 개인정보처리자는 법 제22조제5항에 따라 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명ㆍ연락처에 관한 정보를 수집할 수 있다.<개정 2015.12.30.>

④ 중앙행정기관의 장은 제1항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 "개인정보 보호지침"이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.<개정 2015.12.30.>

제18조(민감정보의 범위) 법 제23조 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보(이하 "고유식별정보"라 한다)를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 「주민등록법」 제7조제3항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제4항에 따른 외국인등록번호

제20조 삭제 <2014.8.6.>

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

③ 행정자치부장관은 기술적ㆍ 경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

[본조신설 2015.12.30.]

제22조(영상정보처리기기 설치ㆍ운영 제한의 예외) ① 법 제25조제2항 단서에서 "대통령령으로 정하는 시설"이란 다음 각 호의 시설을 말한다.

1. 「형의 집행 및 수용자의 처우에 관한 법률」 제2조제4호에 따른 교정시설
2. 「정신보건법」 제3조제3호부터 제5호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당한다), 정신질환자사회복귀시설 및 정신요양시설

② 중앙행정기관의 장은 소관 분야의 개인정보처리자가 법 제25조제2항 단서에 따라 제1항 각 호의 시설에 영상정보처리기기를 설치ㆍ운영하는 경우 정보주체의 사생활 침해를 최소화하기 위하여 필요한 세부 사항을 개인정보 보호지침으로 정하여 그 준수를 권장할 수 있다.

제23조(영상정보처리기기 설치 시 의견 수렴) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치ㆍ운영하려는 공공기관의 장은 다음 각 호의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회ㆍ설문조사 또는 여론조사

② 법 제25조제2항 단서에 따른 시설에 영상정보처리기기를 설치ㆍ운영하려는 자는 다음 각 호의 사람으로부터 의견을 수렴하여야 한다.

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

제24조(안내판의 설치 등) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치ㆍ운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 영상정보처리기기가 설치ㆍ운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 영상정보처리

기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명 및 연락처

② 제1항에도 불구하고 영상정보처리기기운영자가 설치·운영하는 영상정보처리기기가 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 제1항 각 호의 사항을 게재할 수 있다.

1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우

③ 제2항에 따라 인터넷 홈페이지에 제1항 각 호의 사항을 게재할 수 없으면 영상정보처리기기운영자는 다음 각 호의 어느 하나 이상의 방법으로 제1항 각 호의 사항을 공개하여야 한다.

1. 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 "사업장등"이라 한다)의 보기 쉬운 장소에 게시하는 방법
2. 관보(영상정보처리기기운영자가 공공기관인 경우만 해당한다)나 영상정보처리기기운영자의 사업장등이 있는 특별시·광역시·도 또는 특별자치도(이하 "시·도"라 한다) 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법

④ 법 제25조제4항 단서에 따라 공공기관의 장은 다음 각 호의 어느 하나에 해당하는 시설에 설치하는 영상정보처리기기에 대해서는 안내판을 설치하지 아니할 수 있다.<개정 2015.3.11.>

1. 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설
2. 「통합방위법」 제2조제13호에 따른 국가중요시설
3. 「보안업무규정」 제36조에 따른 국가보안시설

제25조(영상정보처리기기 운영·관리 방침) ① 영상정보처리기기운영자는 법 제25조제7항에 따라 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

② 제1항에 따라 마련한 영상정보처리기기 운영·관리 방침의 공개에 관하여는 제31조제2항 및 제3항을 준용한다. 이 경우 "개인정보처리자"는 "영상정보처리기기운영자"로, "법 제30조제2항"은 "법 제25조제7항"으로, "개인정보처리방침"은 "영상정보처리기기 관리·운영 방침"으로 본다.

제26조(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) ① 법 제25조제8항 단서에 따라 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항

3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 제1항에 따라 사무를 위탁한 경우에는 제24조제1항부터 제3항까지의 규정에 따른 안내판 등에 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다.

제27조(영상정보처리기기 설치·운영 지침) 행정자치부장관은 법 및 이 영에서 규정한 사항 외에 영상정보처리기기의 설치·운영에 관한 기준, 설치·운영 사무의 위탁 등에 관하여 법 제12조제1항에 따른 표준 개인정보 보호지침을 정하여 영상정보처리기기운영자에게 그 준수를 권장할 수 있다. <개정 2013.3.23., 2014.11.19.>

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조제1항제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 법 제26조제2항에 따른 수탁자(이하 "수탁자"라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 법 제26조제2항에서 "대통령령으로 정하는 방법"이란 개인정보 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다.

③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.

1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
4. 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

④ 법 제26조제3항 전단에서 "대통령령으로 정하는 방법"이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)을 말한다.

⑤ 위탁자가 과실 없이 제4항에 따른 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 위탁자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.

제29조(영업양도 등에 따른 개인정보 이전의 통지) ① 법 제27조제1항 각 호 외의 부분과 같은 조 제2항 본문에서 "대통령령으로 정하는 방법"이란 서면등의 방법을 말한다.

② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 "영업양도자등"이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 영업양도자등의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

제5장 개인정보의 안전한 관리

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정자치부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.<개정 2013.3.23., 2014.11.19.>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.<개정 2013.3.23., 2014.11.19.>

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① 법 제30조제1항제6호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 처리하는 개인정보의 항목
2. 개인정보의 파기에 관한 사항
3. 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항

② 개인정보처리자는 법 제30조제2항에 따라 수립하거나 변경한 개인정보 처리방침을 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하여야 한다.

③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 수립하거나 변경한 개인정보 처리방침을 공개하여야 한다.

1. 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
4. 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제2항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다.

1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
2. 개인정보 보호 관련 자료의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.<개정 2016.7.22.>

1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원

나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원

다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원

라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장

마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원

바. 시·군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원

사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람

가. 사업주 또는 대표자

나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

③ 행정자치부장관은 개인정보 보호책임자가 법 제31조제2항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다.<개정 2013.3.23., 2014.11.19.>

제33조(개인정보파일의 등록사항) 법 제32조제1항제7호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
3. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
4. 제41조에 따른 개인정보의 열람 요구를 접수·처리하는 부서
5. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

제34조(개인정보파일의 등록 및 공개 등) ① 개인정보파일을 운용하는 공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 행정자치부령으로 정하는 바에 따라 행정자치부장관에게 법 제32조제1항 및 이 영 제33조에 따른 등록사항(이하 "등록사항"이라 한다)의 등록을 신청하여야 한다. 등록 후 등록한 사항이 변경된 경우에도 또한 같다. <개정 2013.3.23., 2014.11.19.>

② 행정자치부장관은 법 제32조제4항에 따라 개인정보파일의 등록 현황을 인터넷 홈페이지에 게재하여야 한다. <개정 2013.3.23., 2014.11.19.>

③ 행정자치부장관은 제1항에 따른 개인정보파일의 등록사항을 등록하거나 변경하는 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영할 수 있다.<개정 2013.3.23., 2014.11.19.>

제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① 행정자치부장관은 제30조제1항 각 호의 사항을 고려하여 개인정보 보호의 관리적·기술적·물리적 보호대책의 수립 등을 포함한 법 제32조의2제1항에 따른 인증의 기준을 정하여 고시한다.

② 법 제32조의2제1항 따라 개인정보 보호의 인증을 받으려는 자(이하 이 조 및 제34조의3에서 "신청인"이라 한다)는 다음 각 호의 사항이 포함된 개인정보 보호 인증신청서(전자문서로 된 신청서를 포함한다)를 제34조의6에 따른 개인정보 보호 인증 전문기관(이하 "인증기관"이라 한다)에 제출하여야 한다.

1. 인증 대상 개인정보 처리시스템의 목록
2. 개인정보 보호 관리체계를 수립·운영하는 방법과 절차

3. 개인정보 보호 관리체계 및 보호대책 구현과 관련되는 문서 목록

③ 인증기관은 제2항에 따른 인증신청서를 받은 경우에는 신청인과 인증의 범위 및 일정 등에 관하여 협의하여야 한다.

④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 서면심사 또는 현장심사의 방법으로 실시한다.

⑤ 인증기관은 제4항에 따른 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 사람을 위원으로 하는 인증위원회를 설치·운영하여야 한다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등 개인정보 보호 인증에 필요한 세부사항은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22.]

제34조의3(개인정보 보호 인증의 수수료) ① 신청인은 인증기관에 개인정보 보호 인증 심사에 소요되는 수수료를 납부하여야 한다.

② 행정자치부장관은 개인정보 보호 인증 심사에 투입되는 인증 심사원의 수 및 인증심사에 필요한 일수 등을 고려하여 제1항에 따른 수수료 산정을 위한 구체적인 기준을 정하여 고시한다.

[본조신설 2016.7.22.]

제34조의4(인증취소) ① 인증기관은 법 제32조의2제3항에 따라 개인정보 보호 인증을 취소하려는 경우에는 제34조의2제5항에 따른 인증위원회의 심의·의결을 거쳐야 한다.

② 행정자치부장관 또는 인증기관은 법 제32조의2제3항에 따라 인증을 취소한 경우에는 그 사실을 당사자에게 통보하고, 관보 또는 인증기관의 홈페이지에 공고하거나 게시하여야 한다.

[본조신설 2016.7.22.]

제34조의5(인증의 사후관리) ① 법 제32조의2제4항에 따른 사후관리 심사는 서면심사 또는 현장심사의 방법으로 실시한다.

② 인증기관은 제1항에 따른 사후관리를 실시한 결과 법 제32조의2제3항 각 호의 사유를 발견한 경우에는 제34조의2제5항에 따른 인증위원회의 심의를 거쳐 그 결과를 행정자치부장관에게 제출하여야 한다.

[본조신설 2016.7.22.]

제34조의6(개인정보 보호 인증 전문기관) ① 법 제32조의2제5항에서 "대통령령으로 정하는 전문기관"이란 다음 각 호의 기관을 말한다.

1. 「정보통신망 이용촉진 및 정보보호에 관한 법률」 제52조에 따른 한국인터넷진흥원(이하 "한국인터넷진흥원"이라 한다)
2. 다음 각 목의 요건을 모두 충족하는 법인, 단체 또는 기관 중에서 행정자치부장관이 지정·고시하는 법인, 단체 또는 기관

가. 제34조의8에 따른 개인정보 보호 인증심사원 5명 이상을 보유할 것

나. 행정자치부장관이 실시하는 업무수행 요건·능력 심사에서 적합하다고 인정받을 것

② 제1항제2호에 해당하는 법인, 단체 또는 기관의 지정과 그 지정의 취소에 필요한 세부기준 등은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22.]

제34조의7(인증의 표시 및 홍보) 법 제32조의2제6항에 따라 인증을 받은 자가 인증 받은 내용을 표시하거나 홍보하려는 경우에는 행정자치부장관이 정하여 고시하는 개인정보 보호 인증표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시하여야 한다.

[본조신설 2016.7.22.]

제34조의8(개인정보 보호 인증심사원의 자격 및 자격 취소 요건) ① 인증기관은 법 제32조의2제7항에 따라 개인정보 보호에 관한 전문지식을 갖춘 사람으로서 인증심사에 필요한 전문 교육과정을 이수하고 시험에 합격한 사람에게 개인정보 보호 인증심사원(이하 "인증심사원"이라 한다)의 자격을 부여한다.

② 인증기관은 법 제32조의2제7항에 따라 인증심사원이 다음 각 호의 어느 하나에 해당하는 경우 그 자격을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 자격을 취소하여야 한다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 취득한 경우
2. 개인정보 보호 인증 심사와 관련하여 금전, 금품, 이익 등을 부당하게 수수한 경우
3. 개인정보 보호 인증 심사 과정에서 취득한 정보를 누설하거나 정당한 사유 없이 업무상 목적 외의 용도로 사용한 경우

③ 제1항 및 제2항에 따른 전문 교육과정의 이수, 인증심사원 자격의 부여 및 취소 등에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22.]

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축ㆍ운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축ㆍ운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축ㆍ운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축ㆍ운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

제36조(영향평가 시 고려사항) 법 제33조제2항제4호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 민감정보 또는 고유식별정보의 처리 여부
2. 개인정보 보유기간

제37조(평가기관의 지정 및 지정취소) ① 행정자치부장관은 법 제33조제1항 후단에 따라 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관(이하 "평가기관"이라 한다)으로 지정할 수 있다. <개정 2013.3.23., 2014.11.19., 2015.12.22.>

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
   가. 영향평가 업무 또는 이와 유사한 업무
   나. 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석ㆍ평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다)
   다. 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
   라. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무
   마. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제8호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
2. 별표 1에 따른 전문인력을 10명 이상 상시 고용하고 있는 법인
3. 다음 각 목의 사무실 및 설비를 갖춘 법인
   가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
   나. 기록 및 자료의 안전한 관리를 위한 설비

② 평가기관으로 지정받으려는 자는 행정자치부령으로 정하는 평가기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다. 이하 같다)를 첨부하여 행정자치부장관에게 제출하여야 한다.<개정 2013.3.23., 2014.11.19.>

1. 정관
2. 대표자 및 임원의 성명
3. 제1항제2호에 따른 전문인력의 자격을 증명할 수 있는 서류
4. 그 밖에 행정자치부령으로 정하는 서류

③ 제2항에 따라 평가기관 지정신청서를 제출받은 행정자치부장관은 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인하여야 한다. 다만, 신청인이 제2호의 확인에 동의하지 아니하는 경우에는 신청인에게 그 서류를 첨부하게 하여야 한다.<개정 2013.3.23., 2014.11.19.>

1. 법인 등기사항증명서
2. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다)

④ 행정자치부장관은 제1항에 따라 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 발급하고, 다음 각 호의 사항을 관보에 고시하여야 한다. 고시된 사항이 변경된 경우에도 또한 같다.<개정 2013.3.23., 2014.11.19.>

1. 평가기관의 명칭·주소 및 전화번호와 대표자의 성명
2. 지정 시 조건을 붙이는 경우 그 조건의 내용

⑤ 행정자치부장관은 제1항에 따라 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소하여야 한다.<개정 2013.3.23., 2014.11.19.>

1. 거짓이나 그 밖의 부정한 방법으로 평가기관의 지정을 받은 경우
2. 지정된 평가기관 스스로 지정취소를 원하는 경우나 폐업한 경우
3. 제1항에 따른 지정요건을 충족하지 못하게 된 경우
4. 제6항에 따른 신고의무를 이행하지 아니한 경우
5. 고의 또는 중대한 과실로 영향평가 업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
6. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우

⑥ 제1항에 따라 지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 행정자치부령으로 정하는 바에 따라 그 사유가 발생한 날부터 7일 이내에 행정자치부장관에게 신고하여야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 30일 이내에 신고하여야 한다.<개정 2013.3.23., 2014.11.19.>

1. 제1항 각 호의 어느 하나에 해당하는 사항이 변경된 경우
2. 제4항제1호에 해당하는 사항이 변경된 경우
3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우

⑦ 행정자치부장관은 제5항에 따라 평가기관의 지정을 취소하려는 경우에는 청문을 하여야 한다.<개정 2013.3.23., 2014.11.19.>

제38조(영향평가의 평가기준 등) ① 법 제33조제6항에 따른 영향평가의 평가기준은 다음 각 호와 같다. <개정 2016.7.22.>

1. 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
2. 법 제24조제3항, 제25조제6항 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성
3. 개인정보 침해의 위험요인별 조치 여부
4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항

② 법 제33조제1항에 따라 영향평가를 의뢰받은 평가기관은 제1항의 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 다음 각 호의 사항이 포함된 평가 결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제35조 각 호에 해당하는 개인정보파일을 구축·운용 또는

변경하기 전에 그 영향평가서를 행정자치부장관에게 제출(영향평가서에 제3호에 따른 개선 필요 사항이 포함된 경우에는 그에 대한 조치 내용을 포함한다)하여야 한다.<개정 2013.3.23., 2014.11.19., 2016.7.22.>

1. 개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적
2. 영향평가 대상 개인정보파일의 개요
3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선이 필요한 사항
4. 영향평가 수행 인력 및 비용

③ 행정자치부장관은 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.<개정 2013.3.23., 2014.11.19.>

제39조(개인정보 유출 신고의 범위 및 기관) ① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 1만명 이상의 정보주체에 관한 개인정보를 말한다.

② 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.<개정 2015.12.30., 2016.7.22.>

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면 등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

② 제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조제1항제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 7일 이상 게시하여야 한다.

제40조의2(과징금의 부과기준 등) ① 법 제34조의2제1항에 따른 과징금의 부과기준은 별표 1의2와 같다.

② 행정자치부장관은 법 제34조의2제1항에 따라 과징금을 부과하려는 경우에는 위반사실, 부과금액, 이의제기 방법 및 이의제기 기간 등을 명시하여 이를 납부할 것을 과징금 부과대상자에게 서면으로 통지하여야 한다.<개정 2014.11.19.>

③ 제2항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 행정자치부장관이 정하는 수납기관에 과징금을 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부하여야 한다.<개정 2014.11.19.>

④ 법 제34조의2제3항 전단에서 "대통령령으로 정하는 가산금"이란 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 매 1개월이 지날 때마다 내지 아니한 과징금의 1천분의 5에 상당하는 금액을 가산한 금액을 말한다.

[본조신설 2014.8.6.]

제6장 정보주체의 권리 보장

제41조(개인정보의 열람절차 등) ① 정보주체는 법 제35조제1항 및 제2항에 따라 자신의 개인정보에 대한 열람을 요구하려는 경우에는 행정자치부령으로 정하는 바에 따라 다음 각 호의 사항 중 열람하려는 사항을 표시한 개인정보 열람요구서를 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23., 2014.11.19.>

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 정보주체가 법 제35조제2항에 따라 행정자치부장관을 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 제1항에 따른 개인정보 열람요구서를 행정자치부장관에게 제출하여야 한다. 이 경우 행정자치부장관은 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송하여야 한다.<개정 2013.3.23., 2014.11.19.>

③ 법 제35조제3항 전단에서 "대통령령으로 정하는 기간"이란 10일을 말한다.

④ 개인정보처리자는 제1항에 따른 개인정보 열람요구서를 받은 날부터 10일 이내에 정보주체에게 해당 개인정보를 열람할 수 있도록 하는 경우와 제42조제1항에 따라 열람 요구 사항 중 일부를 열람하게 하는 경우에는 열람할 개인정보와 열람이 가능한 날짜·시간 및 장소 등(제42조제1항에 따라 열람 요구 사항 중 일부만을 열람하게 하는 경우에는 그 사유와 이의제기방법을 포함한다)을 행정자치부령으로 정하는 열람통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23., 2014.11.19.>

제42조(개인정보 열람의 제한·연기 및 거절) ① 개인정보처리자는 제41조제1항에 따른 열람 요구 사항 중 일부가 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

② 개인정보처리자가 법 제35조제3항 후단에 따라 정보주체의 열람을 연기하거나 같은 조 제4항에 따라 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 연기 또는 거절의 사유 및 이의제기방법을 행정자치부령으로 정하는 열람의 연기·거절 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23., 2014.11.19.>

제43조(개인정보의 정정·삭제 등) ① 정보주체는 법 제36조제1항에 따라 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려는 경우에 행정자치부령으로 정하는 개인정보 정정·삭제 요구서를 해당 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23., 2014.11.19.>

② 다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 개인정보처리자는 법 제36조제1항에 따른 개인정보의 정정 또는 삭제 요구를 받으면 그 요구에 따라 해당 개인정보를 정정·삭제하거나 그 개인정보 정정·삭제 요구서를 해당 개인정보를 제공한 기관의 장에게 지체 없이 보내고 그 처리 결과에 따라 필요한 조치를 하여야 한다.

③ 개인정보처리자는 제1항과 제2항에 따른 개인정보 정정·삭제 요구서를 받은 날부터 10일 이내에 법 제36조제2항에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 경우에는 그 조치를 한 사실을, 법 제36조제1항 단서에 해당하여 삭제 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 행정자치부령으로 정하는 개인정보 정정·삭제 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23., 2014.11.19.>

제44조(개인정보의 처리정지 등) ① 정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려는 경우에 행정자치부령으로 정하는 개인정보 처리정지 요구서를 그 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23., 2014.11.19.>

② 개인정보처리자는 제1항에 따른 개인정보 처리정지 요구서를 받은 날부터 10일 이내에 법 제37조제2항 본문에 따라 해당 개인정보의 처리정지 조치를 한 경우에는 그 조치를 한 사실을, 같은 항 단서에 해당하여 처리정지 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 행정자치부령으로 정하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23., 2014.11.19.>

제45조(대리인의 범위 등) ① 법 제38조에 따라 정보주체를 대리할 수 있는 자는 다음 각 호와 같다.

1. 정보주체의 법정대리인

2. 정보주체로부터 위임을 받은 자

② 제1항에 따른 대리인이 법 제38조에 따라 정보주체를 대리할 때에는 개인정보처리자에게 행정자치부령으로 정하는 정보주체의 위임장을 제출하여야 한다.<개정 2013.3.23., 2014.11.19.>

제46조(정보주체 또는 대리인의 확인) ① 개인정보처리자는 제41조제1항에 따른 열람의 요구, 제43조제1항에 따른 정정·삭제의 요구 또는 제44조제1항에 따른 처리정지의 요구(이하 이 조, 제47조 및 제48조에서 "열람등요구"라 한다)를 받았을 때에는 열람등요구를 한 자가 본인이거나 정당한 대리인인지를 확인하여야 한다.

② 공공기관인 개인정보처리자가 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 제1항에 따른 확인을 할 수 있는 경우에는 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

제47조(수수료 등의 금액 등) ① 법 제38조제3항에 따른 수수료와 우송료의 금액은 열람등요구에 필요한 실비의 범위에서 해당 개인정보처리자가 정하는 바에 따른다. 다만, 개인정보처리자가 지방자치단체인 경우에는 그 지방자치단체의 조례로 정하는 바에 따른다.

② 개인정보처리자는 열람등요구를 하게 된 사유가 그 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구해서는 아니 된다.

③ 법 제38조제3항에 따른 수수료 또는 우송료는 다음 각 호의 구분에 따른 방법으로 낸다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관(이하 이 조에서 "국가기관"이라 한다) 또는 지방자치단체인 개인정보처리자는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 내게 할 수 있다.

1. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
2. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
3. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

제48조(열람 요구 지원시스템의 구축 등) ① 개인정보처리자는 열람등요구 및 그에 대한 통지를 갈음하여 해당 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영하거나 그 밖의 절차를 정하여 해당 업무를 처리할 수 있다.

② 행정자치부장관은 개인정보처리자 중 공공기관이 보유하고 있는 개인정보에 관한 열람등요구 및 그에 대한 통지에 관한 공공기관의 업무 수행을 효율적으로 지원하기 위하여 시스템을 구축·운영할 수 있다.<개정 2013.3.23., 2014.11.19.>

제7장 개인정보 분쟁조정

제48조의2(당연직위원) 법 제40조제1항에 따른 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)의 당연직위원은 행정자치부·방송통신위원회·금융위원회 및 보호위원회의 고위공무원단에 속하는 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 사람 중 소속 기관의 장이 지명하는 사람으로 한다.

[본조신설 2016.7.22.]

제49조(조정부의 구성 및 운영) ① 법 제40조제6항에 따른 조정부(이하 "조정부"라 한다)는 분쟁조정위원회 위원장이 지명하는 5명 이내의 위원으로 구성하되, 그 중 1명은 변호사 자격이 있는 위원으로 한다. <개정 2016.7.22.>

② 분쟁조정위원회 위원장은 조정부의 회의를 소집한다.

③ 분쟁조정위원회의 위원장은 조정부의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

④ 조정부의 장은 조정부 위원 중에서 호선(互選)한다.

⑤ 제1항부터 제4항까지의 규정에서 정한 사항 외에 조정부의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제50조(사무기구) 법 제40조제8항에 따른 분쟁조정 접수 및 사실 확인 등 분쟁조정에 필요한 사무처리는 보호위원회의 사무기구가 수행한다.
[전문개정 2016.7.22.]

제51조(분쟁조정위원회 등의 운영) ① 분쟁조정위원회 위원장은 분쟁조정위원회의 회의를 소집하며, 그 의장이 된다.
② 분쟁조정위원회 위원장이 분쟁조정위원회의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.
③ 분쟁조정위원회 및 조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정되는 경우에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다.

제52조(집단분쟁조정의 신청 대상) 법 제49조제1항에서 "대통령령으로 정하는 사건"이란 다음 각 호의 요건을 모두 갖춘 사건을 말한다.
1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체
다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체
2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것

제53조(집단분쟁조정 절차의 개시) ① 법 제49조제2항 후단에서 "대통령령으로 정하는 기간"이란 14일 이상의 기간을 말한다.
② 법 제49조제2항 후단에 따른 집단분쟁조정 절차의 개시 공고는 분쟁조정위원회의 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문에 게재하는 방법으로 한다.<개정 2015.12.30.>

제54조(집단분쟁조정 절차에 대한 참가 신청) ① 법 제49조에 따른 집단분쟁조정(이하 "집단분쟁조정"이라 한다)의 당사자가 아닌 정보주체 또는 개인정보처리자가 법 제49조제3항에 따라 추가로 집단분쟁조정의 당사자로 참가하려면 법 제49조제2항 후단의 공고기간에 문서로 참가 신청을 하여야 한다.
② 분쟁조정위원회는 제1항에 따라 집단분쟁조정 당사자 참가 신청을 받으면 제1항의 신청기간이 끝난 후 10일 이내에 참가 인정 여부를 문서로 알려야 한다.

제55조(집단분쟁조정 절차의 진행) ① 집단분쟁조정 절차가 개시된 후 제52조제1호가목부터 다목까지의 어느 하나에 해당하게 된 정보주체는 당사자에서 제외된다.
② 분쟁조정위원회는 제52조 각 호의 요건을 모두 갖춘 사건에 대하여 집단분쟁조정 절차가 개시되고 나면 그 후 집단분쟁조정 당사자 중 일부가 같은 조 제1호가목부터 다목까지의 어느 하나에 해당하게 되어 같은 조 제1호의 요건을 갖추지 못하게 되더라도 집단분쟁조정 절차를 중지하지 아니한다.

제56조(수당과 여비) 분쟁조정위원회 및 조정부의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.

제57조(분쟁조정 세칙) 법 및 이 영에서 규정한 사항 외에 분쟁조정위원회의 운영 및 집단분쟁조정을 위하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제8장 보칙 및 벌칙

제58조(개선권고 및 징계권고) ① 법 제61조제2항·제3항에 따른 개선권고 및 법 제65조제2항·제3항에 따른 징계권고는 권고 사항, 권고 사유 및 조치 결과 회신기간 등을 분명하게 밝힌 문서로 하여야 한다.

② 제1항에 따른 권고를 받은 자는 권고 내용에 따라 필요한 조치를 하고, 그 결과를 행정자치부장관 또는 관계 중앙행정기관의 장에게 문서로 통보하여야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보하여야 한다.<개정 2013.3.23., 2014.11.19.>

제59조(침해 사실의 신고 등) 행정자치부장관은 법 제62조제2항에 따라 개인정보에 관한 권리 또는 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위한 전문기관으로 한국인터넷진흥원을 지정한다. <개정 2013.3.23., 2014.11.19.>

제60조(자료제출 요구 및 검사) ① 법 제63조제1항제3호에서 "대통령령으로 정하는 경우"란 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우를 말한다.

② 행정자치부장관은 법 제63조제1항 및 제2항에 따른 자료의 제출 요구 및 검사 등을 위하여 한국인터넷진흥원의 장에게 기술적인 사항을 자문하는 등 필요한 지원을 요청할 수 있다.<개정 2013.3.23., 2014.11.19., 2015.12.30.>

제61조(결과의 공표) ① 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 다음 각 호의 사항을 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문 등에 게재하여 공표할 수 있다. <개정 2013.3.23., 2014.11.19.>

1. 위반행위의 내용
2. 위반행위를 한 자
3. 개선권고, 시정조치 명령, 고발, 징계권고 및 과태료 부과의 내용 및 결과

② 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 제1항 각 호의 사항을 공표하려는 경우에는 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려하여야 한다.<개정 2013.3.23., 2014.11.19.>

③ 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항에 따른 보호위원회에 심의·의결을 요청하기 전에 공표대상자에게 공표대상자라는 사실을 알려 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다.<개정 2013.3.23., 2014.11.19.>

제62조(권한의 위탁) ① 삭제 <2015.12.30.>

② 행정자치부장관은 법 제24조의2제4항에 따른 대체가입수단 제공의 지원에 관한 권한을 다음 각 호의 어느 하나의 기관에 위탁할 수 있다.<개정 2013.3.23., 2014.11.19., 2015.12.30.>

1. 「전자정부법」 제72조제1항에 따른 한국지역정보개발원
2. 한국인터넷진흥원
3. 대체가입수단의 개발·제공·관리 업무를 안전하게 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 행정자치부장관이 고시하는 법인·기관·단체

③ 행정자치부장관은 다음 각 호의 권한을 한국인터넷진흥원에 위탁한다.<개정 2013.3.23., 2014.11.19., 2015.12.30.>

1. 법 제13조제1호에 따른 개인정보 보호에 관한 교육·홍보
2. 법 제33조제5항에 따른 관계 전문가의 육성 및 영향평가 기준의 개발
3. 법 제35조제2항에 따른 열람 요구의 접수 및 처리
4. 법 제63조에 따른 자료제출 요구 및 검사(법 제62조에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 및 상담과 관련된 사항만 해당한다)
5. 제37조제2항에 따른 평가기관 지정신청서의 접수 및 같은 조 제6항에 따른 신고 사항의 접수

④ 행정자치부장관은 제2항에 따라 권한을 위탁하는 경우에는 그 수탁자 및 위탁업무를 고시하여야 한다.<신설 2015.12.30.>

제62조의2(고유식별정보의 처리) ① 행정자치부장관(제62조제3항에 따라 행정자치부장관의 권한을 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2014.11.19., 2015.12.30.>

1. 법 제24조의2제4항에 따른 주민등록번호 대체 방법 제공을 위한 시스템 구축 등 제반 조치 마련 및 지원에 관한 사무
2. 법 제34조의2에 따른 과징금의 부과 및 징수에 관한 사무
3. 법 제62조제3항에 따른 개인정보침해 신고센터의 업무에 관한 사무

② 분쟁조정위원회는 법 제45조 및 제47조에 따른 개인정보 분쟁 조정에 관한 사무를 수행하기 위하여 불가피한 경우 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

[본조신설 2014.8.6.]

제62조의3(규제의 재검토) ① 행정자치부장관은 제40조의2 및 별표 1의2에 따른 과징금의 부과기준 등에 대하여 2014년 1월 1일을 기준으로 3년마다(매 3년이 되는 해의 1월 1일 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

② 행정자치부장관은 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<개정 2015.12.30.>

1. 제23조에 따른 영상정보처리기기 설치 시 의견 수렴: 2015년 1월 1일
2. 제31조에 따른 개인정보 처리방침의 내용 및 공개방법 등: 2015년 1월 1일

2의2. 제37조에 따른 평가기관의 지정 및 지정 취소의 요건 등: 2016년 1월 1일

3. 제41조에 따른 개인정보의 열람절차 등: 2015년 1월 1일
4. 제52조에 따른 집단분쟁조정의 신청 대상: 2015년 1월 1일
5. 제63조 및 별표 2에 따른 과태료의 부과기준: 2015년 1월 1일

[전문개정 2014.12.9.]

제63조(과태료의 부과기준) 법 제75조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 2와 같다.

부칙 <제23169호,2011.9.29.>

제1조(시행일) 이 영은 2011년 9월 30일부터 시행한다. 다만, 제20조 및 별표 2 제2호자목은 2012년 3월 30일부터 시행한다.

제2조(다른 법령의 폐지) 공공기관의 개인정보보호에 관한 법률 시행령을 폐지한다.

제3조(기본계획 및 시행계획의 수립에 관한 경과조치) ① 행정안전부장관은 제11조에도 불구하고 2012년부터 제2014년까지의 기간에 대한 기본계획을 2011년 12월 31일까지 보호위원회의 심의·의결을 거쳐 수립하여야 한다.

② 중앙행정기관의 장은 제12조에도 불구하고 2012년 및 2013년에 시행할 시행계획을 제1항의 기본계획에 따라 2012년 2월 28일까지 보호위원회에 제출하여 2012년 4월 30일까지 보호위원회의 심의·의결을 거쳐 수립하여야 한다.

제4조(개인정보처리자가 수집·보유하고 있는 개인정보의 암호화에 관한 경과조치) 이 영 시행 당시 개인정보를 수집·보유하고 있는 개인정보처리자는 전자매체에 저장하는 개인정보에 대하여 2012년 12월 31일까지 제30조제1항제3호에 따른 암호화 조치(제21조에 따라 준용되는 고유식별정보에 관한 암호화 조치를 포함한다)를 마쳐야 한다.

제5조(개인정보파일의 등록에 관한 경과조치) 이 영 시행 당시 개인정보파일을 운용하고 있는 공공기관(이 영 시행 전에 개인정보파일을 등록한 기관은 제외한다)의 장은 이 영 시행일부터 60일 이내에 제34조에 따라 행정안전부장

관에게 등록을 신청하여야 한다.

제6조(개인정보 영향평가에 관한 경과조치) 이 영 시행 당시 제35조 각 호에 따른 개인정보파일을 운용하고 있거나, 운용할 목적으로 제35조 각 호에 따른 개인정보파일을 구축하고 있는 공공기관의 장은 이 영 시행일부터 5년 이내에 해당 개인정보파일에 대한 영향평가를 실시하고 그 결과를 행정안전부장관에게 제출하여야 한다.

제7조(다른 법령의 개정) ① 가맹사업거래의 공정화에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조의4제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

② 민주화운동관련자 명예회복 및 보상 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제19조의2 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

③ 발명진흥법 시행령 일부를 다음과 같이 개정한다.

제8조의2제2항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

④ 소비자기본법 시행령 일부를 다음과 같이 개정한다.

제25조제7호를 다음과 같이 한다.

7. 「개인정보 보호법」 제40조에 따라 설치된 개인정보 분쟁조정위원회

⑤ 전자정부법 시행령 일부를 다음과 같이 개정한다.

제49조제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제8호"를 "「개인정보 보호법」 제2조제3호"로 한다.

⑥ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제3조제1항 중 "정보통신서비스 제공자 및 제71조에 따른 정보통신서비스 제공자 외의 자"를 "정보통신서비스 제공자"로 한다.

제16조부터 제22조까지를 각각 삭제한다.

제36조제6항을 삭제한다.

제66조제2항 중 "정보통신서비스 제공자등(법 제67조에 따라 준용되는 경우에 해당되는 자를 포함한다)"을 "정보통신서비스 제공자등"으로 한다.

제71조를 삭제한다.

제3조제1항ㆍ제2항, 제66조제2항, 제68조의2제1항 각 호 외의 부분, 같은 조 제2항, 제69조제1항 각 호 외의 부분 후단, 제70조제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 및 별표 9 위반행위란의 제12호 각 목 외의 부분 중 "행정안전부장관 또는 방송통신위원회"를 각각 "방송통신위원회"로 한다.

제8조(다른 법령과의 관계) 이 영 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률 시행령」 또는 그 규정을 인용하고 있는 경우 이 영 가운데 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 영 또는 이 영의 해당 규정을 인용한 것으로 본다.

부칙 <제24425호,2013.3.23.>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ①부터 ④까지 생략

⑤ 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제11조제1항, 같은 조 제2항 전단·후단, 같은 조 제3항, 제12조제1항, 제13조제1항 각 호 외의 부분, 같은 조 제2항, 제14조, 제20조제2항 각 호 외의 부분, 제27조, 제30조제2항·제3항, 제32조제3항, 제34조제1항 전단, 같은 조 제2항·제3항, 제37조제1항 각 호 외의 부분, 제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 본문, 같은 조 제4항 각 호 외의 부분 전단, 같은 조 제5항 각 호 외의 부분 본문, 같은 조 제6항 각 호 외의 부분 본문, 같은 조 제7항, 제38조제2항 각 호 외의 부분, 같은 조 제3항, 제41조제2항 전단·후단, 제48조제2항, 제50조제2항, 제58조제2항 본문, 제59조, 제60조제2항, 제61조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조제1항 각 호 외의 부분, 같은 조 제2항 및 제3항 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

제13조제3항 후단 중 ""행정안전부장관""을 ""안전행정부장관""으로 한다.

제15조 각 호 외의 부분, 제34조제1항 전단, 제37조제2항 각 호 외의 부분, 같은 항 제4호, 같은 조 제6항 각 호 외의 부분 본문, 제41조제1항 각 호 외의 부분, 같은 조 제4항, 제42조제2항, 제43조제1항·제3항, 제44조제1항·제2항 및 제45조제2항 중 "행정안전부령"을 각각 "안전행정부령"으로 한다.

별표 1의 제6호 중 "행정안전부장관"을 "안전행정부장관"으로 한다.

별표 2의 제1호나목1)부터 4)까지 외의 부분 본문 및 같은 호 다목1)부터 3)까지 외의 부분 본문 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

⑥부터 <129>까지 생략

부칙 <제25531호,2014.8.6.>

이 영은 2014년 8월 7일부터 시행한다.

부칙 <제25751호,2014.11.19.>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제5조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <104>까지 생략

<105> 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제11조제1항, 같은 조 제2항 전단·후단, 같은 조 제3항, 제12조제1항, 제13조제1항 각 호 외의 부분, 같은 조 제2항, 같은 조 제3항 후단, 제14조, 제16조제2항, 제27조, 제30조제2항·제3항, 제32조제3항, 제34조제1항 전단, 같은 조 제2항·제3항, 제37조제1항 각 호 외의 부분, 같은 조 제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 본문, 같은 조 제4항 각 호 외의 부분 전단, 같은 조 제5항 각 호 외의 부분 본문, 같은 조 제6항 각 호 외의 부분 본문, 같은 조 제7항, 제38조제2항 각 호 외의 부분, 같은 조 제3항, 제40조의2제2항, 같은 조 제3항 본문, 제41조제2항 전단·후단, 제48조제2항, 제50조제2항, 제58조제2항 본문, 제59조, 제60조제2항, 제61조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조의2제1항 각 호 외의

부분 및 제62조의3 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

제15조 각 호 외의 부분, 제34조제1항 전단, 제37조제2항 각 호 외의 부분, 같은 항 제4호, 같은 조 제6항 각 호 외의 부분 본문, 제41조제1항 각 호 외의 부분, 같은 조 제4항, 제42조제2항, 제43조제1항·제3항, 제44조제1항·제2항 및 제45조제2항 중 "안전행정부령"을 각각 "행정자치부령"으로 한다.

별표 1 제6호 중 "안전행정부장관"을 "행정자치부장관"으로 한다.

별표 2 제1호나목1)부터 4)까지 외의 부분 본문 및 같은 호 다목1)부터 3)까지 외의 부분 본문 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

<106>부터 <418>까지 생략

부칙 <제25840호,2014.12.9.>

제1조(시행일) 이 영은 2015년 1월 1일부터 시행한다.

제2조부터 제16조까지 생략

부칙 <제26140호,2015.3.11.>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제24조제4항제3호 중 "보안목표시설"을 "국가보안시설"로 한다.

②부터 ⑤까지 생략

부칙 <제26728호,2015.12.22.>

제1조(시행일) 이 영은 2015년 12월 23일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제37조제1항제1호라목을 다음과 같이 한다.

라. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무

② 및 ③ 생략

부칙 <제26776호,2015.12.30.>

이 영은 공포한 날부터 시행한다. 다만, 제21조의2, 제62조제2항, 제62조의2제1항제1호 및 별표 2의 개정규정은 2016년 1월 1일부터 시행한다.

부칙 <제27370호,2016.7.22.>

제1조(시행일) 이 영은 2016년 7월 25일부터 시행한다.

제2조(기본계획 및 시행계획의 수립에 관한 경과조치) ① 종전의 제11조에 따라 수립된 2015년부터 2017년까지의 기간에 대한 기본계획은 제11조의 개정규정에 따라 수립된 기본계획으로 본다.

② 종전의 제12조에 따라 수립된 2016년 및 2017년에 대한 시행계획은 각각 제12조의 개정규정에 따라 수립된 시행계획으로 본다.

[별표 1] <개정 2014.11.19.>

전문인력의 자격기준(제37조제1항제2호 관련)

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원이 시행하는 정보보호전문가(SIS) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
2. 「전자정부법」 제60조에 따른 감리원(ISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
3. 「국가기술자격법」에 따른 정보통신 직무분야의 국가기술자격 중 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 전자계산기조직응용기사, 정보처리기사 또는 정보통신기사 기술자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
4. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
5. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
6. 그 밖에 개인정보 보호와 관련된 자격으로서 행정자치부장관이 정하는 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

비고

"개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람"이란 공공기관, 법인 및 단체 등의 임직원으로 개인정보 보호를 위한 공통기반기술(암호기술, 인증기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당하는 분야에서 계획, 분석, 설계, 개발, 운영, 유지·보수, 감리, 컨설팅 또는 연구·개발 업무 등을 수행한 경력이 있는 사람을 말한다.

[별표 1의2] <신설 2014.8.6>

과징금의 부과기준(제40조의2제1항 관련)

1. 과징금 부과 여부의 결정

과징금은 법 제34조의2제2항 각 호의 사항과 위반행위의 내용 등을 종합적으로 고려하여 그 부과 여부를 결정한다. 다만, 법 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 과징금을 부과하지 아니한다.

2. 과징금의 산정기준

과징금은 법 제34조의2제2항 각 호의 사항과 이에 영향을 미치는 사항을 종합적으로 고려하여 산정하되, 가목의 위반 정도에 따른 산정기준액에 나목의 안전성 확보에 필요한 조치 이행 노력 정도 등에 따른 조정(이하 "1차 조정"이라 한다), 다목의 위반행위의 기간 및 횟수 등에 따른 조정(이하 "2차 조정"이라 한다)을 거쳐 라목에 따라 부과과징금을 산정한다. 다만, 산정된 과징금이 5억원을 초과하는 경우에는 5억원으로 한다.

가. 기본 산정기준

위반 정도	산정기준액	비 고
매우 중대한 위반행위	3억 5천만원	고의 또는 중과실로 인하여 10만건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 "분실등"이라 한다)된 경우를 말한다.
중대한 위반행위	2억 3천만원	고의 또는 중과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우 및 경과실로 인하여 10만건 이상의 주민등록번호가 분실등이 된 경우를 말한다.
일반 위반행위	1억원	경과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우를 말한다.

나. 1차 조정

법 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도, 피해를 최소화하기 위한 대책 마련 등 피해확산 방지를 위한 후속조치 이행 여부를 고려하여 산정기준액의 100분의 50의 범위에서 가중하거나 감경한다.

다. 2차 조정

위반행위의 기간 및 횟수, 위반 행위에 대한 조사 협조 여부, 위반행위에 따른 추가적 피해 발생 여부, 평소 개인정보 보호를 위한 노력 정도 등을 종합적으로 고려하여 1차 조정된 금액의 100분의 50의 범위에서 가중하거나 감경한다.

라. 부과과징금의 산정

개인정보처리자의 현실적 부담능력이나 그 위반행위가 미치는 효과, 위반행위로 인하여 취득한 이익의 규모 등을 고려하여 볼 때 과중하다고 인정되는 경우에는 2차 조정된 금액의 100분의 50의 범위에서 감액하여 부과과징금으로 정할 수 있다.

[별표 2] <개정 2016. 7. 22.>

과태료의 부과기준(제63조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료를 부과받은 경우에 적용한다. 이 경우 위반행위에 대하여 과태료 부과처분을 한 날과 다시 같은 위반행위를 적발한 날을 각각 기준으로 하여 위반 횟수를 계산한다.

나. 행정자치부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우

2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우

3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우

4) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우

다. 행정자치부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개인 경우라도 법 제75조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용 및 정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우

2) 법 위반상태의 기간이 3개월 이상인 경우

3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제15조제1항을 위반하여 개인정보를 수집한 경우	법 제75조제1항제1호	1000	2000	4000
나. 법 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조제2항제1호	600	1200	2400

다. 법 제16조제3항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조제2항제2호	600	1200	2400
라. 법 제20조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조제2항제3호	600	1200	2400
마. 법 제21조제1항을 위반하여 개인정보를 파기하지 않은 경우	법 제75조제2항제4호	600	1200	2400
바. 법 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조제3항제1호	200	400	800
사. 법 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 경우	법 제75조제3항제2호	200	400	800
아. 법 제22조제5항을 위반하여 법정대리인의 동의를 받지 않은 경우	법 제75조제1항제2호	1000	2000	4000
자. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조제2항제4호의2	600	1200	2400
차. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조제2항제4호의3	600	1200	2400
카. 법 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조제2항제5호	600	1200	2400
타. 법 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조제2항제6호	600	1200	2400
파. 법 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조제2항제7호	600	1200	2400
하. 법 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조제1항제3호	1000	2000	4000
거. 법 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 않은 경우	법 제75조제3항제3호	200	400	800
너. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 않은 경우	법 제75조제3항제4호	200	400	800
더. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조제3항제5호	200	400	800
러. 법 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은 경우	법 제75조제3항제6호	200	400	800

머. 법 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조제3항제7호	200	400	800
버. 법 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조제3항제8호	500		
서. 법 제32조의2제6항을 위반하여 인증을 받지 않았음에도 거짓으로 인증의 내용을 표시하거나 홍보한 경우	법 제75조제2항제7호의2	600	1200	2400
어. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조제2항제8호	600	1200	2400
저. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조제2항제9호	600	1200	2400
처. 법 제35조제3항을 위반하여 열람을 제한하거나 거절한 경우	법 제75조제2항제10호	600	1200	2400
커. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조제3항제9호	200	400	800
터. 법 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조제2항제11호	600	1200	2400
퍼. 법 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조제2항제12호	600	1200	2400
허. 법 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우	법 제75조제3항제10호			
1) 자료를 제출하지 않은 경우		100	200	400
2) 자료를 거짓으로 제출한 경우		200	400	800
고. 법 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조제3항제11호	200	400	800
노. 법 제64조제1항에 따른 시정명령에 따르지 않은 경우	법 제75조제2항제13호	600	1200	2400

개인정보 보호법 시행규칙

[시행 2014.11.19.] [행정자치부령 제1호, 2014.11.19., 타법개정]

행정자치부 (개인정보보호정책과) 02 - 2100 - 4105

제1조(목적) 이 규칙은 「개인정보 보호법」 및 같은 법 시행령에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 공공기관은 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공(이하 "목적외이용등"이라 한다)하는 경우에는 「개인정보 보호법」(이하 "법"이라 한다) 제18조제4항에 따라 개인정보를 목적외이용등을 한 날부터 30일 이내에 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 게재하여야 한다. 이 경우 인터넷 홈페이지에 게재할 때에는 10일 이상 계속 게재하되, 게재를 시작하는 날은 목적외이용등을 한 날부터 30일 이내여야 한다.

1. 목적외이용등을 한 날짜
2. 목적외이용등의 법적 근거
3. 목적외이용등의 목적
4. 목적외이용등을 한 개인정보의 항목

제3조(개인정보 보호업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.

② 법 제32조제1항과 영 제34조제1항에 따른 개인정보파일 등록 신청 및 변경등록 신청은 별지 제2호서식의 개인정보파일 등록·변경등록 신청서에 따른다.

③ 영 제37조제2항에 따라 개인정보 영향평가기관의 지정을 신청하려는 자는 별지 제3호서식의 개인정보 영향평가기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 행정자치부장관에게 제출하여야 한다.<개정 2013.3.23., 2014.11.19.>

1. 영 제37조제2항제1호부터 제3호까지의 규정에 따른 서류
2. 영 제37조제2항제4호에 따른 다음 각 목의 서류
   가. 별지 제4호서식의 개인정보 영향평가 수행인력 보유 현황
   나. 별지 제5호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황
   다. 영 제37조제1항제1호의 사실을 증명할 수 있는 서류 등 행정자치부장관이 정하는 서류
3. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(영 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부한다)

④ 법 제33조제1항과 영 제37조제4항에 따른 개인정보 영향평가기관 지정서는 별지 제6호서식과 같다.

⑤ 법 제33조제6항과 영 제37조제6항에 따른 신고는 별지 제7호서식의 개인정보 영향평가기관 변경사항 신고서에 따른다.

⑥ 법 제35조제1항·제2항과 영 제41조제1항에 따른 개인정보 열람의 요구, 법 제36조제1항과 영 제43조제1항에 따른 개인정보 정정·삭제 요구, 법 제37조제1항과 영 제44조제1항에 따른 개인정보 처리정지 요구는 별지 제8호서식의 개인정보 열람, 정정·삭제, 처리정지 요구서에 따른다.

⑦ 법 제35조제5항과 영 제41조제4항에 따른 개인정보 열람 및 일부열람의 통지, 법 제35조제3항 후단과 영 제42조제2항에 따른 개인정보 열람연기의 통지, 법 제35조제4항과 영 제42조제2항에 따른 열람거절의 통지는 별지 제9호서식의 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서에 따른다.

⑧ 법 제36조제6항과 영 제43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조제5항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.

⑨ 영 제45조제2항에 따른 정보주체의 위임장은 별지 제11호서식과 같다.

부칙 <제241호,2011.9.29.>

제1조(시행일) 이 규칙은 2011년 9월 30일부터 시행한다.

제2조(다른 법령의 폐지) 공공기관의 개인정보보호에 관한 법률 시행규칙은 폐지한다.

제3조(다른 법령과의 관계) 이 규칙 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률 시행규칙」 또는 그 규정을 인용하고 있는 경우 이 규칙 가운데 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 규칙 또는 이 규칙의 해당 규정을 인용한 것으로 본다.

부칙 <제1호,2013.3.23.>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 개인정보 보호법 시행규칙 일부를 다음과 같이 개정한다.

제3조제3항 각 호 외의 부분 및 같은 항 제2호다목 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

별지 제2호서식, 별지 제3호서식, 별지 제6호서식 및 별지 제7호서식 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

별지 제3호서식의 처리절차란 중 "행정안전부"를 각각 "안전행정부"로 한다.

②부터 <51>까지 생략

부칙 <제1호,2014.11.19.>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 시행규칙 중 이 규칙 시행 전에 공포되었으나 시행일이 도래하지 아니한 시행규칙을 개정한 부분은 각각 해당 시행규칙의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ① 개인정보 보호법 시행규칙 일부를 다음과 같이 개정한다.

제3조제3항 각 호 외의 부분 및 같은 항 제2호다목 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

별지 제2호서식, 별지 제3호서식, 별지 제6호서식 및 별지 제7호서식 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

별지 제3호서식의 처리절차란 중 "안전행정부"를 각각 "행정자치부"로 한다.

②부터 <42>까지 생략

■ 개인정보 보호법 시행규칙 [별지 제1호서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="3">[ ] 목적외 이용 [ ] 제3자 제공</td></tr>
<tr><td>목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td></td><td rowspan="3">담당자</td><td>소 속
성 명
전화번호</td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td rowspan="3">담당자</td><td>성 명
소 속
전화번호</td></tr>
<tr><td>이용하거나 제공한 날짜,
주기 또는 기간</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한 형태</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공의 법적
근거</td><td colspan="3"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="3"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라
제한을 하거나 필요한
조치를 마련할 것을
요청한 경우에는 그 내용</td><td colspan="3"></td></tr>
</table>

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제2호서식] <개정 2014.11.19.>

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처리기간 7일

공공기관 명칭	주소	등록부서	전화번호

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

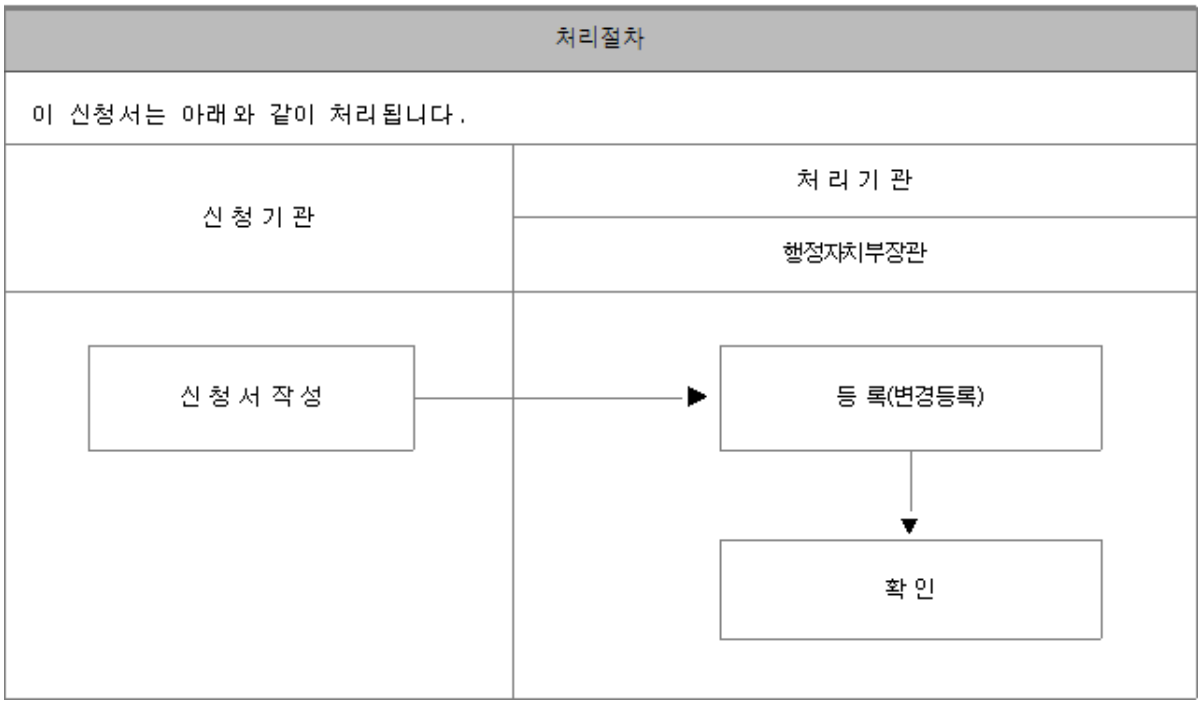
년 월 일

신청기관 (서명 또는 인)

행정자치부장관 귀하

210mm×297mm[일반용지 70g/㎡(재활용품)]

(뒤 쪽)



■ 개인정보 보호법 시행규칙 [별지 제3호서식] <개정 2014.11.19.>

개인정보 영향평가기관 지정신청서

접수번호	접수일	처리기간 2개월

신청인	법인명 및 대표자 성명	법인 설립일
	소재지	전화번호
개인정보 영향평가 수행인력의 수	명	

「개인정보 보호법 시행령」 제37조제2항에 따라 개인정보 영향평가기관 지정을 위와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

행정자치부장관 귀하

첨부서류	1. 「개인정보 보호법 시행령」 제37조제2항제1호부터 제3호까지의 규정에 따른 서류 2. 「개인정보 보호법 시행령」 제37조제2항제4호에 따른 다음의 서류 가. 「개인정보보호법 시행규칙」 별지 제4호서식의 개인정보 영향평가 수행인력 보유 현황 나. 「개인정보보호법 시행규칙」 별지 제6호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황 다. 「개인정보 보호법 시행령」 제37조제1항제1호의 사실을 증명할 수 있는 서류 등 행정자치부장관이 정하는 서류 3. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(「개인정보보호법 시행령」 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부합니다)

처리절차

신청서 작성	→	접 수	→	검 토	→	결 재	→	지정서 발급
신청인		처 리 기 관 (한국정보화진흥원)		처 리 기 관 (행정자치부)		처 리 기 관 (행정자치부)		

210㎜×297㎜[일반용지 70g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제4호서식]

개인정보 영향평가 수행인력 보유현황

법인명 및 대표자 성명								
영향평가 수행인력 총수			명					
일련번호	성명	생년월일	입사일	보유자격증 (취득연월일)	자격증 취득 후 업무 수행 경력 (년 개월)	전문분야	학위 및 학과	비고

유의사항
전문분야는 「개인정보보호법 시행령」 제37조제1항제1호 각 목에 따른 업무 분야를 말합니다.

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제5호서식]

개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황

※ 아래의 작성방법을 읽고 작성하시기 바랍니다.

법인명 및 대표자 성명	
소 재 지	

① 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실

[ ] 있음 [ ] 없음

② 신원 확인 및 출입 통제 설비

명 칭	설비 등의 세부사항	수 량	비고

③ 기록 및 자료의 안전관리 설비

명 칭	설비 등의 세부사항	수 량	비 고

작 성 방 법

①의 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실이 있는 경우에는 '있음'란에 [√] 표시를 하고, 없는 경우에는 '없음'란에 [√] 표시를 합니다.

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제6호서식] <개정 2014.11.19.>

제 호

개인정보 영향평가기관 지정서

1. 대 표 자:
2. 생년월일 또는 사업자등록번호:
3. 법 인 명:
4. 주 소:
5. 전화번호:
6. 지정요건:

「개인정보 보호법」 제33조제1항과 같은 법 시행령 제37조제4항에 따라 위의 법인을 개인정보 영향평가기관으로 지정하였으므로 개인정보 영향평가기관 지정서를 발급합니다.

년 월 일

행정자치부장관 직인

210㎜×297㎜[보존용지 120g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제7호서식] <개정 2014.11.19.>

개인정보 영향평가기관 변경사항 신고서

접수번호	접수일자	처리기간 7일

신고인	법인명		
	대표자명	생년월일	
	주소 (주된 사무소의 소재지) (전화번호 :)		
변경일			
구분	종 전	변 경	
수행 인력			
사무실 및 설비			
평가 기관 양도·양수 또는 합병 등	종전 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
	변경 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
법인 명칭·주소·전화번호 및 대표자 변경			

「개인정보 보호법」 제33조제6항과 같은 법 시행령 제37조제6항에 따라 평가기관의 변경사항을 위와 같이 신고합니다.

년 월 일

신고인 대표 (서명 또는 인)

행정자치부장관 귀하

첨부서류	1. 양도·양수·합병 등의 경우 양도·양수 또는 합병 계약서 등 사본 1부 2. 그 밖의 변경사항 증명서류 각 1부

유의사항
위 변경사항과 관련하여 자세한 내용은 별지로 작성하거나 관련 서류를 첨부하여 제출할 수 있습니다.

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제8호서식]

개인정보([ ] 열람 [ ] 정정·삭제 [ ] 처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 10일 이내

정보주체	성 명	전 화 번 호	
	생년월일		
	주 소		
대리인	성 명	전 화 번 호	
	생년월일	정보주체와의 관계	
	주 소		
요구내용	[ ] 열람	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용	
	[ ] 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.	
	[ ] 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.	

「개인정보 보호법」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

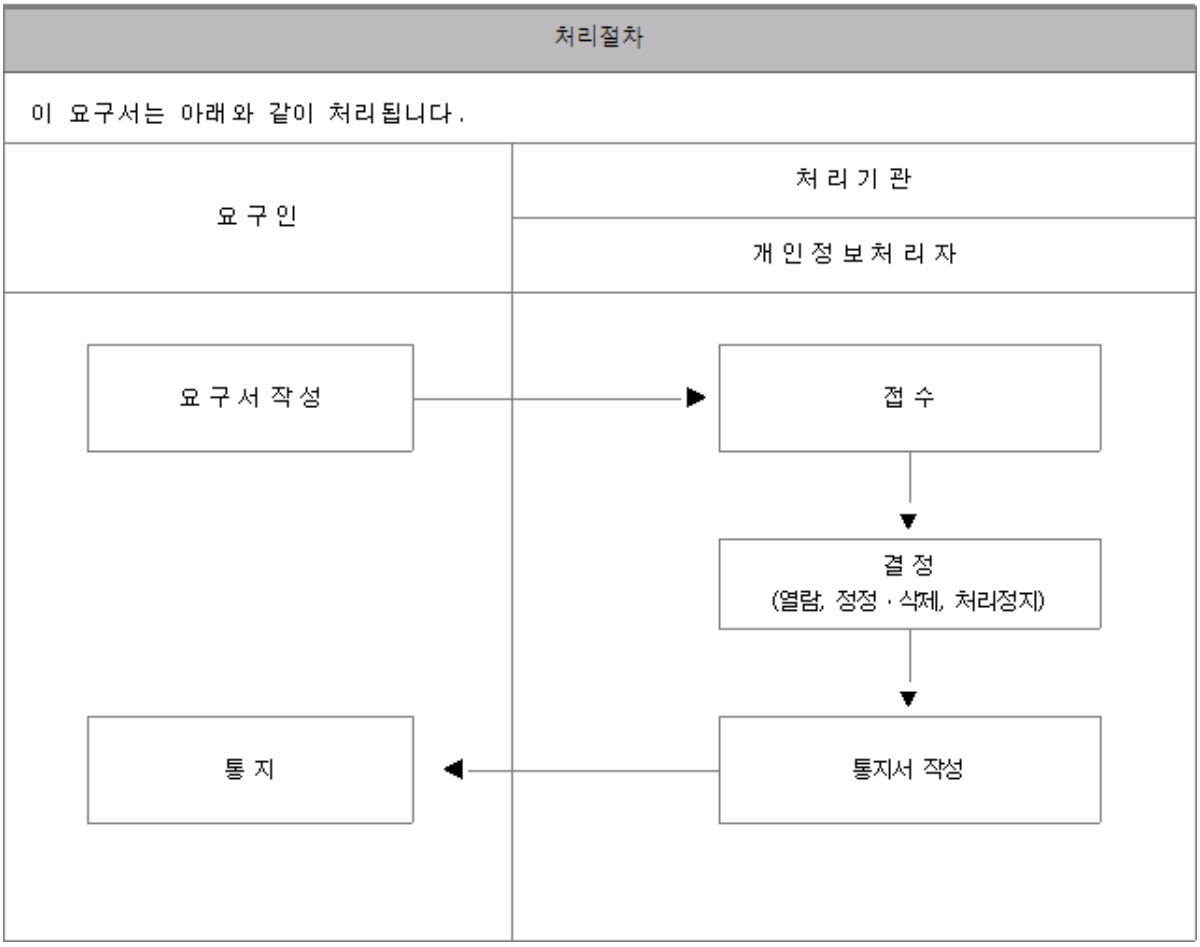
○○○○ 귀하

작 성 방 법

1. '대리인'란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 '열람' 란에 [√] 표시를 하고 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 '정정·삭제' 란에 [√] 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 '처리정지' 란에 [√] 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.

210mm×297mm[일반용지 70g/㎡(재활용품)]

(뒤 쪽)


처리절차
이 요구서는 아래와 같이 처리됩니다.
요 구 인
처 리 기 관
개 인 정 보 처 리 자
요 구 서 작 성
접 수
결 정
(열람, 정정 · 삭제, 처리정지)
통 지
통지서 작성

■ 개인정보 보호법 시행규칙 [별지 제9호서식]

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용						
열람 일시		열람 장소				
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)						
열람 형태 및 방법	열람 형태	[ ]열람·시청	[ ]사본·출력물	[ ]전자파일	[ ]복제물·인화물	[ ]기타
	열람 방법	[ ]직접방문	[ ]우편	[ ]팩스	[ ]전자우편	[ ]기타
납부 금액	①수수료 원	②우송료 원	계(①+②) 원			
	수수료 산정 명세					
사 유						
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.					

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

210㎜×297㎜[신문용지 54g/㎡]

(뒤 쪽)

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.

가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)

나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서

2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.

가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지

나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지

다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.

3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제10호서식]

개인정보 ([ ] 정정·삭제, [ ] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제11호서식]

위 임 장

위임받는 자	성명	전 화 번 호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (□ 열람, □ 정정·삭제, □ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자 (서명 또는 인)

O O O O 귀하

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

행정자치부 예규, 훈령, 고시

「표준 개인정보보호 지침(고시)」

◉ 행정자치부 고시 제2016-21호

표준 개인정보 보호지침

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 처리"란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회·동창회 등 비영리기관·단체, 개인 등을 말한다.
3. "공공기관"이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제2조에 따른 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을

말한다.

7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.
8. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 영 제3조에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
9. "개인영상정보"란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.
10. "영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.
⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

제2장 개인정보 처리 기준

제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.
② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가

능하거나 현저히 곤란한 경우

4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우

5. 개인정보를 수집·이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

6. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제7조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.
② 법 제17조의 "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).
③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제8조(개인정보의 목적 외 이용·제공) ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.
② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.
③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.
④ 개인정보처리자가 법 제18조제2항제4호에 따라 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제9조(개인정보 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니 하다.

1. 고지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제10조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.

제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하

여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.
② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제12조(동의를 받는 방법) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 정보주체의 동의는 동의가 필요한 개인정보에 한한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.
② 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 법 제18조제3항 각 호의 사항을 알리고 동의를 받아야 한다.

1. 개인정보를 수집·이용하고자 하는 경우로서 법 제15조제1항제2호 내지 제6호에 해당하지 않은 경우
2. 법 제18조제2항에 따라 개인정보를 수집 목적 외의 용도로 이용하거나 제공하고자 하는 경우
3. 법 제22조제3항에 해당하여 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우
4. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우

③ 개인정보처리자는 제2항 각 호에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.
④ 개인정보처리자는 법 제15조제1항제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.
⑤ 개인정보처리자가 영 제17조제1항제2호의 규정에 따라 전화에 의한 동

의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑥ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑦ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 「개인정보 수집·제공 동의서 작성 가이드라인」을 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조제3항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.
② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 당해 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.
③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제17조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.

제3절 개인정보 처리방침 작성

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확

하게 표현하여야 한다.
② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당하는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)
7. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자에 관한 사항
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도

"개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제4절 개인정보 보호책임자

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제3항에 따라 행정자치부장관이 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제2항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제24조(교육계획의 수립 및 시행) ① 행정자치부장관은 매년 초 당해 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.
② 행정자치부장관은 제1항의 교육계획에 따라 사단법인 한국개인정보보호협의회 등의 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.
③ 행정자치부장관은 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받은 수 있는 여건 조성을 위해 노력하여야 한다.

제5절 개인정보 유출 통지 및 신고 등

제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

제26조(유출 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할

수 있는 방법 등에 관한 정보

4. 개인정보처리자의 대응조치 및 피해구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실

2. 제1항의 통지항목 중 확인된 사항

③ 개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출 사고가 발생한 시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제26조제1항 각 호의 사항을 공개할 수 있다.

제28조(개인정보 유출신고 등) ① 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치 결과를 5일 이내에 행정자치부장관 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 영 제39조제2항에 따른 전문기관의 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제26조제1항의 사항을

신고한 후, 별지 제1호서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제26조제1항에 따른 통지와 함께 인터넷 홈페이지 등에 정보주체가 알아보기 쉽도록 제26조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로

판단되는 경우 신고의 종결 처리

5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제6절 정보주체의 권리 보장

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.
② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제3장 영상정보처리기기 설치·운영

제1절 영상정보처리기기의 설치

제35조(적용범위) 이 장은 영상정보처리기기운영자가 공개된 장소에 설치·운영하는 영상정보처리기기와 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제36조(영상정보처리기기 운영·관리 지침) ① 영상정보처리기기 운영·관리 지침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.
② 영상정보처리기기 운영·관리 지침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니하거나, 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.

제37조(관리책임자의 지정) ① 영상정보처리기기운영자는 개인영상정보

의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.
② 제1항의 관리책임자는 법 제31조제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.
1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무
③ 법 제31조에 따른 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인정보 보호책임자가 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 영상정보처리기기운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.
1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처
② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제2절 개인영상정보의 처리

제40조(개인영상정보 이용·제3자 제공 등 제한 등) ① 영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제41조(보관 및 파기) ① 영상정보처리기기운영자는 수집한 개인영상정

보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 지체 없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

② 영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽

게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제27조에 따른 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.
② 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제3절 개인영상정보의 열람등 요구

제44조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 "열람등"이라 한다)을 해당 영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.
② 영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.
③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.
④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)
2. 개인영상정보의 보관기간이 경과하여 파기한 경우
3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항 및 제6항에 따른 기록 및 관리는 별지 제3호서식에 따른 '개인영상정보 관리대장'을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제4절 개인영상정보 보호 조치

제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 '소상공인'은 내부관리계획을 수립하지 아니할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 행정자치부장관에게 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 공공기관의 장은 제1항과 제3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

③ 공공기관 외의 영상정보처리기기운영자는 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체

점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

제4장 공공기관 개인정보파일 등록·공개

제1절 총칙

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」,「고등교육법」및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일
2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일

가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일

나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일

다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일

라. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일

마. 다른 법령에 따라 비밀로 분류된 개인정보파일

3. 법 제58조제1항에 따라 적용이 제외되는 다음 각목의 개인정보파일

가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일

나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일

다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일

4. 영상정보처리기기를 통하여 처리되는 개인영상정보파일

5. 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일

6.「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 행정자치부에 등록하여야 한다.

② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 행정자치부에 직접 등록하여야 한다.

③ 교육청 및 각급 학교 등은 교육부를 통하여 행정자치부에 등록하여야 한다.

④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 행정자치부에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 보호법 시행규칙」(이하 "시행규칙"이라 한다) 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서‘를 활용할 수 있다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리 방법
7. 개인정보의 보유 기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

③ 개인정보취급자는 등록한 사항이 변경된 경우에는 시행규칙 제3조제2항에 따른 별지 제2호서식의 '개인정보파일 등록·변경등록 신청서'를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 행정자치부에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 행정자치부에 등록하여야 한다.

③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 행정자치부에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방

자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 '개인정보파일 표준목록'에 따라 등록해야 한다.
② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙부처에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.
③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.
④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록 사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.
② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 행정자치부에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는 제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고

판단되는 경우에는 개선을 권고할 수 있다.

② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제53조제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 행정자치부장관은 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 행정자치부장관은 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 행정자치부장관은 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 ‘개인정보 목적 외 이용·제공대장’에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.
② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과「공공기록물 관리에 관한 법률 영」에 따른 기록관리기준표를 상회할 수 없다.
③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속하여 보유할 수 있다.

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.
② 행정자치부장관은 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.
③ 행정자치부는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

제5장 보칙

제62조(친목단체에 대한 벌칙조항의 적용배제) ① 친목단체의 개인정보처리자에 대하여는 법 제75조제1항제1호, 법 제75조제2항제1호, 법 제75조제3항제7호 및 법 제75조제3항제8호의 벌칙을 적용하지 아니한다.
② 제1항에서 규정한 사항을 제외한 벌칙규정은 친목단체의 개인정보처리자에 대하여도 적용한다.

제63조(처리 중인 개인정보에 관한 경과조치) ① 법 시행 전에 근거법령 없이 개인정보를 수집한 경우 당해 개인정보를 보유하는 것은 적법한 처리로 본다. 다만, 이 법 시행 이후 기존의 수집목적 범위 내에서 이용하는 경우를 제외하고 개인정보를 새롭게 처리하는 경우에는 법, 영, 시행규칙 및 이 지침에 따라야 한다.

② 법 시행 전에 법률의 근거 또는 정보주체의 동의 없이 제3자로부터 개인정보를 제공받아 목적 외의 용도로 이용하고 있는 개인정보처리자는 정보주체의 동의를 받아야 한다.

③ 법 시행 전에 개인정보를 수집한 개인정보처리자는 기존의 수집목적 범위에도 불구하고 제1항 단서 및 제2항을 준수하기 위하여 새롭게 정보주체의 동의를 받을 목적으로 법 시행 전에 수집한 개인정보를 이용할 수 있다.

부칙<제2016-00호,2016.6.00.> 이 규정은 발령한 날부터 시행한다.

[별지 제1호서식]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

[별지 제2호서식] (앞 쪽)

개인영상정보(□ 존재확인 □ 열람) 청구서 ※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.	처리기한 10일 이내

청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	영상정보 기록기간	(예 : 2011.01.01 18:30 ~ 2011.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			

「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

○ ○ ○ ○ 귀하

담당자의 청구인에 대한 확인 서명	

[별지 제3호서식]

개인영상정보 관리대장

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

[별지 제4호서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제5호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지 제6호서식]

개인정보 목적 외 이용·제공 대장

구분	주요내용
① 개인정보파일명	
② 이용·제공받는 기관	
③ 이용·제공일자	
④ 이용·제공주기	
⑤ 이용·제공형태	
⑥ 이용·제공목적	
⑦ 이용·제공근거	
⑧ 이용·제공항목	
⑨ 비고	

[별표 1호]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

개인정보의 안전성 확보조치 기준

제정 2011. 9.30. 행정안전부고시 제2011-43호
개정 2014.12.30. 행정자치부고시 제2014- 7호

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "소상공인"이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.
5. "중소사업자"란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업·제조업·건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.
7. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
9. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
10. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준을 말한다.
12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.
17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

제3조(내부관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을

업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는

개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제9조(물리적 접근 방지) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

부칙<제2011-43호, 2011. 9. 30.>

제1조 이 기준은 고시한 날부터 시행한다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치·운영 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙<제2014-7호, 2014. 12. 30.>

이 기준은 고시한 날부터 시행한다.

행정자치부고시 제2015-53호

제정 2011.9.30 행정안전부장관고시 제2011-39호
개정 2012.12.26 행정안전부장관고시 제2012-59호
개정 2015.12.31 행정자치부장관고시 제2015-53호

개인정보 영향평가에 관한 고시

제1장 총 칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제33조와 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제38조에 따른 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음과 각 호와 같다.

1. "개인정보 영향평가(이하"영향평가"라 한다)"란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.
3. "개인정보 영향평가기관(이하 "평가기관"이라 한다)"이란 영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 행정자치부장관이 지정한 기관을 말한다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.

5. "개인정보 영향평가 관련 분야 수행실적(이하 "영향평가 관련 분야 수행실적"이라 한다)"이란 영 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

제2장 개인정보 영향평가기관의 지정

제3조(평가기관 지정절차) ① 영 제37조에 따른 평가기관의 지정절차는 지정신청 공고, 지정신청 서류 접수 및 검토, 현장실사, 종합심사의 순으로 진행된다.

② 행정자치부장관은 평가기관으로 지정받으려는 자가 지정 신청을 할 수 있도록 관보 등을 통해 15일 이상 지정신청공고를 하여야 한다.

③평가기관으로 지정받으려는 자는 「개인정보 보호법 시행규칙」(이하 "규칙"이라 한다) 별지 제3호 서식의 "개인정보 영향평가기관 지정신청서"와 함께 다음 각 호의 서류를 행정자치부장관에게 제출한다.

1. 별지 제1호서식의 개인정보 영향평가 수행실적 명세서
2. 별지 제2호서식의 개인정보 영향평가 수행실적물 관리가드
3. 별지 제3호서식의 개인정보 영향평가 수행인력의 경력 및 실적 증명서
4. 별지 제4호서식의 개인정보 영향평가 수행인력 관리카드
5. 별지 제5호서식의 개인정보 영향평가 수행능력 세부 심사자료
6. 별지 제6호서식의 개인정보 영향평가 관련 기술자산 보유목록

④ 행정자치부장관은 제3항에 따른 평가기관 지정신청을 받은 경우 지정기준의 적합여부를 심사하기 위하여 평가기관 지정심사위원회(이하 "지정심사위원회"라 한다)를 구성・운영한다.

⑤ 행정자치부장관은 현장실사와 종합심사를 통해 지정심사위원회의 심사결과를 검증하고, 영향평가 수행인력의 자격요건을 확인한 후 평가기관을 확정한다.

⑥ 평가기관의 유효기간은 행정자치부장관이 평가기관으로 지정한 날로부터 2년으로 한다.

⑦ 평가기관의 유효기간을 연장하고자 하는 자는 유효기간 만료일 3개월 전까지 제3조제3항에 따른 서류를 행정자치부장관에게 제출해야 한다.

제4조(지정심사위원회의 구성 및 운영) ① 제3조에 따른 지정심사위원회는 다음 각 호의 자격을 가진 자 중에서 행정자치부장관이 위촉하는 15인 이내의 위원으로 구성한다.

1.「고등교육법」제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 8년 이상인 사람

2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 8년 이상 개인정보 보호 업무에 종사한 사람

3. 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람

② 지정심사위원회는 영 제37조제1항에 따른 신청한 법인의 자격 및 업무수행능력 등을 검토한다.

③ 지정심사위원회의 위원 임기는 2년으로 하되, 연임할 수 있다.

④ 지정심사위원회의 회의는 필요에 따라 행정자치부장관이 소집한다.

제5조(영향평가 수행인력 자격) ① 영향평가 수행인력은 다음 각 호와 같이 일반수행인력과 고급수행인력으로 구분할 수 있다.

1. 일반수행인력의 자격은 다음 각 목과 같다.

가. 영 제37조제1항제2호의 전문인력 자격을 갖춘 사람

나. 한국CPO포럼이 시행하는 개인정보관리사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야 수행실적이 있는 사람

2. 고급수행인력의 자격은 다음 각 목과 같다.

가. 제1호의 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행실적이 있는 사람

나. 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

다. 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

② 제1항에 따른 영향평가수행인력은 제6조제2항에 따른 전문교육을 이수하고 제6조제3항에 따른 전문인력 인증서를 받은 경우에 영향평가를 수행할 수 있다.

제6조(영향평가 전문교육의 운영 및 실시) ① 행정자치부장관은 영향평가 전문인력 양성을 위한 세부 교육계획 수립 및 교육 운영 등의 업무를 효율적으로 추진하기 위하여 한국인터넷진흥원을 전문교육기관으로 지정한다.

② 전문교육기관의 장은 영향평가 전문인력양성을 위한 세부 교육계획을 수립하여 전문교육 등을 실시하여야 한다.

③ 전문교육기관의 장은 전문교육 이수자에 대한 평가를 실시하고 그 결과에 따라 개인정보 영향평가 전문인력 인증서를 교부한다.

④ 전문교육기관의 장은 다음 각 호의 1에 해당되는 경우에는 제3항에 따른 전문인력 인증서를 교부받은 자에 대한 계속교육을 실시하여야 하며, 이수여부에 따라 전문인력 인증서를 갱신하여 교부한다.

1. 인증서를 교부받은 후 매 2년이 경과한 경우

2. 법령 또는 평가기준 등의 개정에 따른 변경사항이 발생하여 교육의 실시가 필요하다고 판단되는 경우

⑤ 제3항 또는 제4항에 따라 전문인력 인증서를 교부받은 자가 전문교육기관의 장이 정하는 기간내에 제4항의 계속교육을 이수하지 아니하여 인증서를 갱신하지 못한 경우 기존 인증서의 효력은 상실된다.

제7조(영향평가 수행능력심사의 세부평가 및 지정기준) ① 평가기관의 영향평가 수행능력심사의 세부평가기준은 별표 1과 같다.

② 행정자치부장관은 영향평가 수행능력심사 세부평가기준에 따른 심사결과가 총점 75점 이상인 경우 신청한 법인을 평가기관으로 지정한다.

③ 평가기관의 유효기간을 연장하고자 하는 자에 대한 세부평가기준은 별표 2와 같다.

제8조(사후관리) ① 행정자치부장관은 평가기관이 영 제37조제1항의 평가기관 지정요건을 충족하는 지 여부와 영 제37조제6항에 따른 변경사항을 확인하기 위하여 현장실사, 관련 자료제출 요구 등을 할 수 있다.

② 평가기관은 다음 각 호를 포함한 보호대책을 별표 3과 같이 수립·시행하여야 하며, 행정자치부장관은 그에 대한 준수여부를 점검할 수 있다.

1. 영향평가 수행구역 및 설비에 대한 보호대책
2. 영향평가 수행 인력에 대한 보호대책
3. 문서 및 전산자료에 대한 보호대책
4. 일반 관리적 보호대책

③ 행정자치부장관은 평가기관이 영 제37조제5항제3호부터 제6호까지의 규정에 해당하는 경우에는 지정취소 이전에 시정 및 보완을 요구할 수 있다.

제3장 개인정보 영향평가의 절차 등

제9조(평가절차) 대상기관은 다음 각 호와 같이 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행한다.

1. 사전 준비 단계에서는 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정한다.
2. 영향평가 수행 단계에서는 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성한다.
3. 이행 단계에서는 영향평가서의 침해요인에 대한 개선계획이 반영되는 가를 점검한다.

제10조(평가영역 및 평가분야) 영 제38조제1항의 영향평가기준에 따른 평가영역은 별표 4와 같다. 다만, 대상기관이 1년 이내에 다른 정보시스템의 영향평가를 받은 경우에는 대상기관의 개인정보보호 관리체계에 대한 평가는 생략할 수 있다.

제11조(평가항목) ① 평가기관은 별표 4에 따라 적합한 평가항목을 선정하여 영향평가를 수행하여야 한다. 다만, 대상기관이 1년 이내에 이미 평가받은 항목은 그 변경이 없는 때에는 평가항목에서 제외된다.

② 별표 4에 명시되지 않은 특화된 IT기술을 적용하는 경우에는 해당 기술이 개인정보 보호에 미치는 영향에 대한 평가항목을 개발하여 영향평가 시 반영하여야 한다.

제12조(영향평가서의 제출) 영 제38조제2항에 따라 영향평가서를 제출받은 대상기관의 장은 2개월 이내에 평가결과에 대한 내부승인 절차를 거쳐 영향평가서를 행정자치부장관에게 제출하여야 한다.

제13조(영향평가 수행안내서) 행정자치부장관은 영향평가에 필요한 세부기준 및 절차, 평가항목 등을 구체화하는 "영향평가 수행안내서"를 마련하여 제공할 수 있다.

제14조(영향평가서 개선계획의 이행) 영 제38조제2항에 따라 영향평가서를 제출받은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행 현황을 영향평가서를 제출받은 날로부터 1년 이내에 행정자치부장관에게 제출하여야 한다.

부 칙<제2015-53호, 2015.12.31.>

제1조(시행일) 이 고시는 고시한 날부터 시행한다.

제2조(재검토 기한) 행정자치부장관은「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시에 대하여 2016년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일 까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

■ 개인정보 영향평가에 관한 고시 [별표 1]

개인정보 영향평가 수행능력심사 세부평가기준 (제7조 관련)

구분	평가항목	세부평가항목	배점	평가지표	세부 평가 기준
Ⅰ. 정량 평가 (60)	1.경험 (25)	최근 5년간 영향평가 관련 분야 수행실적	15	계약금액 총액	· 5억원 이상: 배점의 100% · 5억원 미만: 배점의 χ% ※ χ = (계약금액총액/5억원) × 100
		최근 2년간 계약금액 1천만원 이상의 영향평가 관련 분야 수행실적	10	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 χ% ※ χ = (수행건수/5건) × 100
	2.전문성 (25)	고급수행인력의 수	15	인원수	· 인원수 × 1점(최대 15점)
		개인정보 영향평가 전문교육 인증시험 합격자 수	10	비율	· 배점 × (개인정보보호 전문교육 인증시험 합격자 수/ 전체 평가기관 인증시험 평균 합격자 수*) ※ 평가기관 인증시험 합격자수 평균
	3. 신뢰도 (10)	신용평가등급	10	등급	· 신용평가 등급에 근거하여 평가 ※ 개인정보 영향평가에 관한 고시 별표1의 붙임기준
Ⅱ. 정성 평가 (40)	영향평가 수행역량 (40)	영향평가 수행실적의 질적 평가	20	비계량	· 영향평가 품질제고 활동 · 영향평가 수행 대상기관 · 영향평가 수행방법의 우수성
		영향평가 수행인력의 자질 및 경험	10	비계량	※ 신청서류, 현장실사 등을 통해 평가

Ⅱ. 정성평가 (40)	영향평가 수행역량 (40)	지정신청법인의 자체 개인정보영향평가대책	10	비계량	· 위험분석의 타당성 · 개인정보영향평가의 적절성 · 개인정보영향평가의 실효성
Ⅲ. 기타		「벤처기업육성에 관한 특별조치법」 제25조에 따라 벤처기업으로 확인을 받은 기업	가점	확인여부	※ 벤처 확인기업: 가점 5점
		지방소재(수도권제외) 기업	가점	확인여부	※ 본사 위치가 수도권을 제외한 지방에 위치하는 경우 : 가점 5점
		최근 3년간 조달법령에 따라 부정당업자로 지정되어 입찰참가가 제한을 받은 기간	감점	입찰참가 제한월수	※ 제한월수 1월당: 감점 0.5점

비 고

1. 위 표 각 세부 평가항목별 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 세부 평가기준 중 신뢰도 항목은 기업신용평가서 제출로 대체할 수 있으며 이에 대한 배점기준은 [붙임] 신용평가등급에 의한 평가기준에 따른다.
3. '최근'의 기산일은 지정공고일자를 기준으로 한다.

■ 개인정보 영향평가에 관한 고시 [별표 2]

개인정보 영향평가기관 갱신 세부평가기준 (제7조 관련)

구분	평가항목	세부평가항목	배점	평가지표	세부 평가 기준
Ⅰ. 정량 평가 (60)	1.경험 (30)	최근 2년간 영향평가 수행실적	10	계약금액 총액	· 3억원 이상: 배점의 100% · 3억원 미만 : 배점의 χ% ※ χ = (계약금액총액/3억원) × 100
		최근 2년간 영향평가 수행건수	10	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 χ% ※ χ = (수행건수/5건) × 100
		최근 2년간 영향평가 관련 분야 수행실적	5	계약금액 총액	· 5억원 이상 : 배점의 100% · 5억원 ~ 2억원 : 배점의 χ% · 2억원 미만 : 자격미달(시행령 제37조 제1항 제1호) ※ χ = (계약금액총액/5억원) × 100
			5	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 χ% ※ χ = (수행건수/5건) × 100
	2.전문성 (20)	고급수행인력의 수	10	인원수	· 10명 이상 : 배점의 100% · 10명 미만 : 배점의 x% ※ x = (고급인력 총수/10명) x 100%
		개인정보 영향평가 전문교육 인증시험 합격자 수	10	비율	· 배점 × (개인정보보호 전문교육 인증시험 합격자 수/ 전체 평가기관 인증시험 평균 합격자 수*) ※ 평가기관 인증시험 합격자수 평균
	3. 신뢰도 (10)	신용평가등급	10	등급	· 신용평가 등급에 근거하여 평가 ※ 개인정보 영향평가에 관한 고시 별표1의 붙임기준
Ⅱ. 정성 평가 (40)	1.영향 평가 수행 역량 (40)	영향평가 수행실적의 질적 평가	20	비계량	· 영향평가 품질제고 활동 · 영향평가 수행 대상기관 · 영향평가 수행방법의 우수성
		영향평가 수행인력의 자질 및 경험(인터뷰)	10	비계량	※ 신청서류, 현장실사 등을 통해 평가

Ⅱ. 정성 평가 (40)	1.영향 평가 수행 역량 (40)	지정신청법인의 자체 개인정보 영향평가 대책	10	비계량	· 위험분석의 타당성 · 개인정보영향평가의 적절성 · 개인정보영향평가의 실효성
Ⅲ. 기타		「벤처기업육성에 관한 특별조치법」 제25조에 따라 벤처기업으로 확인을 받은 기업	가점	확인여부	※ 벤처 확인기업: 가점 5점
		지방소재 공공기관에 대한 영향평가 수행 건수	가점	확인여부	※ 수행 건수 당 : 가점 1점
		무자격자를 활용한 영향평가 수행 건수 (고시 제5조 위반 건수)	감점	확인여부	※ 수행 건수 당 : 감점 1점
		최근 3년간 조달법령에 따라 부정당업자로 지정되어 입찰참가가 제한을 받은 기간	감점	입찰참가 제한월수	※ 제한월수 1월당: 감점 0.5점

비 고

1. 위 표 각 세부 평가항목별 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 세부 평가기준 중 신뢰도 항목은 기업신용평가서 제출로 대체할 수 있으며 이에 대한 배점기준은 [붙임] 신용평가등급에 의한 평가기준에 따른다.
3. '최근'의 기산일은 지정공고일자를 기준으로 한다.

[붙임]

신용평가등급에 의한 평가기준

회사채에 대한 신용평가등급	기업어음에 대한 신용평가등급	기업신용평가 등급	평점(점)
			10점
AAA	–	AAA (회사채에 대한 신용평가등급 AAA에 준하는 등급)	10.0
AA+, AA0, AA–	A1	AA+, AA0, AA– (회사채에 대한 신용평가등급 AA+, AA0, AA–에 준하는 등급)	
A+	A2+	A+ (회사채에 대한 신용평가등급 A+에 준하는 등급)	
A0	A20	A0 (회사채에 대한 신용평가등급 A0에 준하는 등급)	
A–	A2–	A– (회사채에 대한 신용평가등급 A–에 준하는 등급)	
BBB+	A3+	BBB+ (회사채에 대한 신용평가등급 BBB+에 준하는 등급)	8.0
BBB0	A30	BBB0 (회사채에 대한 신용평가등급 BBB0에 준하는 등급)	
BBB–	A3–	BBB– (회사채에 대한 신용평가등급 BBB–에 준하는 등급)	
BB+, BB0	B+	BB+, BB0 (회사채에 대한 신용평가등급 BB+, BB0에 준하는 등급)	7.0
BB–	B0	BB– (회사채에 대한 신용평가등급 BB–에 준하는 등급)	
B+, B0, B–	B–	B+, B0, B– (회사채에 대한 신용평가등급 B+, B0, B–에 준하는 등급)	6.0
CCC+ 이하	C 이하	CCC+ 이하 (회사채에 대한 신용평가등급 CCC+에 준하는 등급)	3.0

■ 개인정보 영향평가에 관한 고시 [별표 3]

개인정보 영향평가기관 보호대책의 주요 내용 (제8조 관련)

항 목	주 요 내 용
Ⅰ. 영향평가 수행구역 및 설비에 대한 보호대책	1. 영향평가를 수행하는 구역을 지정하여야 한다. 이 구역은 해당 영향평가 수행인력이 아닌 자의 출입이 제한되어야 한다. 2. 영향평가 분석자료를 처리·전송·저장하는 정보통신망에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 이 경우 노트북 컴퓨터, 그 밖에 휴대용 정보처리기기에 대한 통제대책을 포함하여야 한다.
Ⅱ. 영향평가 수행인원에 대한 보호대책	3. 영향평가 수행인력이 관계법령에 따르는 비밀유지의무를 포함한 제반의무를 숙지하고 이의 준수를 확약하는 내용의 서약서를 작성하는 지침과 절차를 마련하여야 한다. 4. 영향평가 수행인력을 채용할 때의 적격 심사와 퇴직할 때의 퇴직자 관리를 위한 지침과 절차를 마련하여야 한다. 5. 영향평가 수행인력이 평가기관의 보안대책을 위반하는 경우의 제재 및 처리에 관한 내부규정을 마련하여야 한다. 6. 영향평가 수행인력을 포함한 임직원이 정기적으로 업체 내부 및 외부의 개인정보 영향평가 교육을 받을 수 있도록 하여야 한다.
Ⅲ. 문서 및 전산자료에 대한 보호대책	7. 영향평가 분석자료(부수자료를 포함한다)를 보호하기위하여 법 제12조의 표준개인정보 보호지침에 따른 보안대책을 마련하여야 한다. 8. 영향평가 수행인력이 아닌 자는 영향평가 분석자료에 접근·열람하거나 편집·반출·폐기하지 못하도록 통제대책을 강구하여야 한다. 9. 정보통신망을 통하여 처리·전송·저장하는 영향평가 분석자료에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 10. 서면, 도면, 마이크로필름·전산출력물 등 출력물 형태의 영향평가 분석자료에 대한 보관·복사·배포·폐기 등에 관한 통제대책을 강구하여야 한다.
Ⅳ. 일반 관리 대책	11. 영향평가에 관한 평가기관의 기본방침을 대표자가 서면으로 공표하고 영향평가 수행인력을 포함한 임직원이 이를 숙지하여야 한다. 12. 영향평가업무에 대한 위험분석 및 통제대책의 관리·운영실태를 주기적으로 점검·평가하여야 한다.

■ 개인정보 영향평가에 관한 고시 [별표 4]

개인정보 영향평가의 평가영역 및 평가분야 (제10조～제11조 관련)

평가 영역	평가 분야	세부 분야
Ⅰ. 대상 기관 개인정보보호 관리 체계	1. 개인정보보호 조직	개인정보보호책임자의 지정
		개인정보보호책임자 역할수행
	2. 개인정보보호 계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내
		유출사고 대응
	4.정보주체권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법 안내
Ⅱ. 대상시스템의 개인정보보호 관리 체계	5.개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
		개인정보파일 등록
	7. 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
Ⅲ. 개인정보처리단계별 보호 조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
	10.이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	11. 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성

IV. 대상시스템의 기술적 보호 조치	13. 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
		출력시 보호조치
	21.개인정보처리구역보호	보호구역지정
V. 특정 IT기술 활용시 개인정보보호	22. CCTV	CCTV 설치시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 바이오정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항

■ 개인정보 영향평가에 관한 고시 [별지 제1호서식]

개인정보 영향평가 관련 분야 수행실적 명세서

업체명						
기간						
수행실적 총계				외 건 (총 천원)		
일련 번호	프로젝트명 (대상기관 (기업)명)	수행기간 (총참여 M/M)	과제책임자	금액 (천원)	참여인력 (개인별 참여율 (M/M), 전문참여분야)	비고 (기반시설 여부, 영향평가 지분 등)

비고

1. 영향평가 관련 분야 수행실적은 개인정보 영향평가 수행실적, 정보보호컨설팅 수행실적, 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기), 감리수행실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기) 등을 말한다.
2. 영향평가 관련 분야 수행실적 명세서는 영향평가 관련 분야를 수행하였던 대상기관에서 작성하되 부득이한 경우 대상기관과의 계약서, 사업완료보고서, 납품증명서, 준공조서 등으로 대체할 수 있다.
3. 영향평가 관련 분야 수행실적 세부사항은 영향평가 관련 분야 수행실적을 간략히 확인할 수 있도록 금액규모를 구분하여 영향평가 수행실적, 정보보호컨설팅 수행건수 및 금액(또는 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 건수 및 금액비율, 감리수행실적 중 정보보호컨설팅 건수 및 금액 비율)을 표기한다.

영향평가 관련 분야 수행실적 세부사항

영향평가 실적 / 금액규모	영향평가 관련 분야 수행건수 (합계)	영향평가 관련 분야 수행금액 (합계)	영향평가 수행건수	영향평가 수행금액	영향평가 건수비율	영향평가 금액비율
1억원 이상						
5천만원 이상						
3천만원 이상						
1천만원 이상						
계/평균비율						

비고

1. 영향평가 관련 분야 수행실적은 개인정보 영향평가 수행실적, 정보보호컨설팅 수행실적, 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기), 감리수행실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기) 등을 말한다.
2. 영향평가 관련 분야 수행실적 명세서는 영향평가 관련 분야를 수행하였던 대상기관에서 작성하되 부득이한 경우 대상기관과의 계약서, 사업완료보고서, 납품증명서, 준공조서 등으로 대체할 수 있다.
3. 영향평가 관련 분야 수행실적 세부사항은 영향평가 관련 분야 수행실적을 간략히 확인할 수 있도록 금액규모를 구분하여 영향평가 수행실적, 정보보호컨설팅 수행건수 및 금액(또는 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 건수 및 금액비율, 감리수행실적 중 정보보호컨설팅 건수 및 금액 비율)을 표기한다.

■ 개인정보 영향평가에 관한 고시 [별지 제2호서식]

개인정보 영향평가 수행실적물 관리카드

업 체 명					
수행 실적물 관리번호	수행 실적물명	수행 실적물 생성일	대상기관명	수행 실적물 폐기일(방법)	비고

비고

1. 개인정보 영향평가 수행실적물이란 개인정보 영향평가를 수행한 평가결과보고서를 말한다.

210㎜×297㎜[일반용지60g/㎡(재활용품)]

■ 개인정보 영향평가에 관한 고시 [별지 제3호서식]

개인정보 영향평가 수행인력의 경력 및 실적 증명서

※ 이 서식은 「개인정보 보호법 시행령」 제37조에 따른 개인정보영향평가기관 지정심사에 활용됨

인적 사항	성 명 (한 자)		생년월일		
	주 소				
경력 사항	근 무 부 서	근무 기간	직위(직급)	담 당 업 무 (구체적으로 기재)	
실적 사항	프로젝트명	수행기간	대상기관명	담당자 전화 번호	비고

본 증명서의 기재 사항에 일체 허위사실이 없음을 확인하오며 허위 사실 기재로 인한 불이익에는 이의를 제기하지 않겠습니다.

년 월 일

신 청 인 (서명 또는 인)

행정자치부장관 귀하

210㎜×297㎜[일반용지 70g/㎡(재활용품)]

■ 개인정보 영향평가에 관한 고시 [별지 제4호서식]

개인정보 영향평가 수행인력 관리카드

(제1쪽)

법인명			
성명		생년월일	
소속부서명			
주소			
입사일		인력등재일	
퇴사일		인력삭제일	
인력구분 : 일반 / 고급		등급 취득일 :	등급 변경기록 :

	기관명(학교명)	기 간	소 속 부 서 (직위, 직책)	자 격 명 (취득일)	비고
학력 및 이력 사항					

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 영향평가에 관한 고시 [별지 제5호서식]

개인정보 영향평가 수행능력 세부 심사자료

Ⅰ. 총매출액 대비 개인정보 영향평가 관련 분야 매출액의 비율

(1) 지정신청직전 결산회기의 총매출액: 천원

(2) 지정신청직전 결산회기의 개인정보영향평가 관련 분야의 매출액: 천원

(3) 총매출액 대비 개인정보 영향평가 관련 분야 매출액의 비율: %

Ⅱ. 부채비율 및 자기자본이익율

(1) 부채비율 = (부채총계 / 자본총계) × 100 = %

(2) 자기자본이익율 = (당기순이익 / 평균자기자본) × 100 = %

Ⅲ. 기 타

(1) 「벤처기업육성에 관한 특별조치법」에 따른 벤처기업 확인 여부 (○ , ×)

(2) 조달관계법령에 따른 부정당업자 지정 경험 여부 (○ , ×)

비 고

1. Ⅰ항, Ⅱ항은 공인회계사 또는 지정신청업체 회계담당자가 서명날인한 계산내역을 첨부한다 (개인정보 영향평가 관련 분야 매출액을 정확하게 확정할 수 없는 경우에는 개산한 금액으로 한다).

■ 개인정보 영향평가에 관한 고시 [별지 제6호서식]

개인정보 영향평가 관련 기술자산 보유목록

법 인 명						
순번	기술자산명	기술자산 버전	기술자산 용도	기술자산 생성일	폐기일 (방법)	비고

비고

1. 기술자산이란 개인정보 영향평가 컨설팅관련 특허, 시스템 개발, 프로그램 개발 등을 말한다.

210㎜×297㎜[일반용지60g/㎡(재활용품)]

■ 개인정보 영향평가에 관한 고시 [별지 제7호서식]

개인정보 영향평가서 개요

<table>
<tr><td colspan="2">공공기관 명</td><td colspan="5"></td></tr>
<tr><td rowspan="5">평가대상시스템 개요</td><td>시스템명</td><td colspan="3"></td><td>추진 일정</td><td></td></tr>
<tr><td>추진개요 및 목적</td><td colspan="5"></td></tr>
<tr><td rowspan="3">추진성격</td><td>대상여부</td><td colspan="2"></td><td rowspan="2">추진예산</td><td rowspan="2"></td></tr>
<tr><td>추진주체</td><td colspan="2"></td></tr>
<tr><td>추진근거</td><td colspan="2"></td><td>비고</td><td></td></tr>
<tr><td>주요내용</td><td colspan="5"></td></tr>
<tr><td rowspan="6">개인정보 파일 개요</td><td>개인정보 수집 목적</td><td colspan="5"></td></tr>
<tr><td rowspan="5">평가대상 파일</td><td>파일명</td><td>정보주체수</td><td colspan="3">파일 및 범위 설명</td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td>...</td><td>...</td><td colspan="3"></td></tr>
<tr><td>주요 개인정보 수집 현황</td><td colspan="5">o 총 ( )개 항목 :
- 필수 수집 :
- 선택 수집 :</td></tr>
<tr><td rowspan="3">영향평가 항목</td><td rowspan="3">주요 평가항목 변경 내역 (수행안내서 78개 지표 활용 내역 기술)</td><td></td><td colspan="4">주요내용</td></tr>
<tr><td>지표추가 항목</td><td colspan="4">-</td></tr>
<tr><td>지표삭제 항목</td><td colspan="4">-</td></tr>
<tr><td rowspan="6">평가결과 및 개선계획</td><td rowspan="3">평가결과 및 개선사항</td><td>주요내용</td><td colspan="5">○</td></tr>
<tr><td colspan="2">침해요인 도출건수</td><td>개선대책 도출건수</td><td>개선계획 수립건수</td><td>조치완료 건수</td><td>조치예정 건수</td></tr>
<tr><td colspan="2">건</td><td>건</td><td>건</td><td>건</td><td>건</td></tr>
<tr><td colspan="2" rowspan="3">주요개선 계획 및 일정</td><td colspan="5">○</td></tr>
<tr><td colspan="5">○</td></tr>
<tr><td colspan="5">○</td></tr>
<tr><td>평가기관</td><td></td><td>평가기간</td><td></td><td>평가예산</td><td></td></tr>
</table>

210㎜×297㎜[일반용지60g/㎡(재활용품)]

■ 개인정보 영향평가에 관한 고시 [별지 제8호서식]

개인정보 영향평가서 개선계획 이행점검 확인서

평가영역	개선과제명	개선요구내용	조치계획	완료일 (또는 예정일)	담당자 확인

◉ 행정자치부 고시 제2015-52호

개인정보 보호 인증제 운영에 관한 규정 전부 개정

개인정보 보호 인증제 운영에 관한 규정을 다음과 같이 전부 개정한다.

개인정보보호 관리체계 인증 등에 관한 고시

제 1 장 총칙

제1조(목적) 이 고시는 「개인정보 보호법」제13조제3호 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제47조의3제2항에 따른 개인정보보호 관리체계 인증에 관하여 필요한 사항을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보보호 관리체계 인증"이란 신청기관의 개인정보보호를 위한 일련의 조치와 활동이 인증심사 기준에 부합하다고 승인하는 것을 말한다.
2. "개인정보보호 관리체계 인증기관(이하 '인증기관'이라 한다)"이란 인증에 관한 업무를 수행할 수 있도록 「개인정보 보호법」 제13조제3호의 업무 수행을 위해 행정자치부가 정하는 전문기관 및 정보통신망법 제47조의3 제3항 및 정보통신망법 제47조제5항에 따라 방송통신위원회가 지정하는 기관을 말한다.
3. "업무수행 요건·능력 심사"란 인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 개인정보보호 관리체계가 별표 5의 개인정보보호 관리체계 인증기준에 적합한 지의 여부를 '한국인터넷진흥원'(이하 '인터넷진흥원'이라 한다) 또는 인증기관이 서면심사

및 현장심사의 방법으로 확인하는 것을 말한다.

5. "개인정보보호 관리체계 인증위원회(이하 '인증위원회'이라 한다)"란 인터넷진흥원 또는 인증기관의 장이 인증심사 결과 등을 심의·의결하기 위해 설치·운영하는 기구로서 위원장과 위원으로 구성된다.

6. "인증심사원"이란 인터넷진흥원으로부터 자격을 부여받고 인증심사를 수행하는 자를 말한다.

7. "신청기관"이란 인터넷진흥원 또는 인증기관에 개인정보보호 관리체계 인증을 신청한 자를 말한다.

8. "최초심사"란 처음으로 인증을 신청하거나 인증범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

9. "사후심사"란 인증을 취득한 기관이 수립하여 운영 중인 개인정보보호 관리체계가 인증기준에 적합하고 지속적으로 유지되고 있는 지를 확인하기 위하여 인증 유효기간 중에 매년 1회 이상 시행하는 인증심사를 말한다.

10. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 개인정보보호 관리체계 인증기관

제3조(인증기관 등) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 업무를 수행한다.

1. 인증심사의 실시 및 인증·인증취소
2. 인증서 발급, 인증마크의 교부 및 인증사실의 관리
3. 인증위원회의 구성·운영
4. 인증심사기준 및 인증심사기법의 연구개발
5. 인증심사원의 자격인정, 교육·승급 및 인증심사 경력의 관리
6. 인증제도 관련 연구 및 동향 조사·분석, 그밖에 인증제도의 운영에 필요한 사항

② 행정자치부와 방송통신위원회는 인증기관을 지정할 필요가 있는 때에는 협의하여 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

③ 제2항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 행정자치부 또는 방송통신위원회에 제출하여야 한다.

1. 별지 제1호 서식의 개인정보보호 관리체계 인증기관 지정 신청서
2. 별지 제2호 서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(인증기관의 지정기준 및 지정절차 등) ① 인증기관에 대한 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 행정자치부와 방송통신위원회는 제3조제3항에 따라 인증기관의 지정 신청을 받은 때에는 협의하여 제1항에 따라 업무수행요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

③ 행정자치부와 방송통신위원회는 협의하여 업무수행 요건·능력을 심사하고 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.

④ 행정자치부와 방송통신위원회는 협의하여 심사 결과를 바탕으로 하여 인증기관으로의 지정여부를 최종 결정한다.

⑤ 행정자치부와 방송통신위원회는 인증기관으로 지정된 신청인에게 별지 제3호의 개인정보보호 관리체계 인증기관 지정서를 발급한다.

⑥ 인증기관의 유효기간은 3년으로 한다.

제5조(인증기관의 사후관리) 인증기관은 매년 2월말까지 전년도의 인증실적을 별지 제4호 서식의 인증실적 보고서에 작성하여 행정자치부와 방송통신위원회에 제출하여야 한다.

제6조(인증기관 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 3개월 전까지 별지 제1호 서식에 따라 행정자치부 또는 방송통신위원회에 재지정 신청을 할 수 있다.

② 행정자치부와 방송통신위원회는 제1항에 따라 재지정 신청을 받은 때에는 협의하여 재지정 여부를 결정한다.

제3장 인증심사원의 자격 및 관리

제7조(인증심사원의 자격 요건 등) ① 인증심사원의 등급별 자격 요건은 별표 3과 같다.

② 인증심사원은 인증심사 수행능력에 따라 심사원보, 심사원, 선임심사원으로 구분한다.

제8조(인증심사원 자격 신청) ① 인증심사원이 되려는 자는 인터넷진흥원이 시행하는 인증심사원 양성교육 과정을 수료하고 평가에 합격하여야 한다.

② 심사원 자격을 신청하고자 하는 자는 인터넷진흥원이 공고하는 신청기간 내에 별지 제5호 서식의 개인정보보호 관리체계 인증심사원 자격 신청서와 관련 서류를 제출하여야 한다.

제9조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합여부를 확인하여 통과한 자에게 별지 제6호 서식의 인증심사원 자격 증명서를 발급하여야 한다.

제10조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 만료 전까지 인터넷진흥원 또는 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수하여야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제11조(인증심사원 자격 취소) 인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원 자격을 취소할 수 있다.

1. 인증심사원 자격 신청 시 제출한 서류가 허위인 경우
2. 인증심사 수행 중 취득한 정보를 관련 법령의 근거나 신청기관의 동의 없이 타인에게 누설하거나 업무목적 외에 이를 사용한 경우
3. 인증심사와 관련된 일체의 금전, 금품, 이익 등을 부당하게 수수한 경우

제4장 인증심사의 신청 및 계약

제12조(신청기관의 사전 준비사항) ① 개인정보보호 관리체계 인증을 받고자 하는 신청기관은 개인정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 개인정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

② 신청기관은 인증심사를 위하여 다음 각 호의 사항을 인증심사 실시 전에 준비하여야 한다.

1. 인증심사를 위한 관련 문서 및 증거자료 등의 열람제공
2. 인증심사를 수행하기 위하여 필요한 장소·시설·장비·기자재 등의 확보
3. 그밖에 인증심사를 원활하게 수행하기 위하여 인터넷진흥원 또는 인증기관이 요구하는 사항

제13조(인증 신청 등) ① 인증을 취득하고자 하는 신청기관은 다음 각 호의 어느 하나에 해당하는 유형의 인증을 신청할 수 있다.

1. 「소상공인 보호 및 지원에 관한 법률」제2조제1호 및 제2호에 따른 소상공인에 해당하는 사업자 및 그 밖의 사업자(유형1)
2. 「중소기업기본법」제2조에 따른 중소기업에 해당하는 사업자(유형2)
3. 「대·중소기업 상생협력 촉진에 관한 법률」제2조제2호에 따른 대기업에 해당하는 사업자 및 정보통신망법 제2조제2호에 따른 “정보통신서비스 제공자”(유형3)
4. 「개인정보 보호법」제2조제6호에 따른 공공기관(유형4)

② 제1항에 따라 인증을 신청하는 기관은 인증의 대상을 특정 서비스·업무로 구분하여 신청하여야 한다.

③ 제1항에 따라 인증을 신청하고자 하는 기관은 별지 제7호 서식의 개인정보보호 관리체계 인증 신청서 및 인증심사와 관련되는 다음 각 호의 사항을 인터넷진흥원 또는 인증기관에 제출하여야 한다.

1. 인증범위 내의 개인정보 처리시스템의 목록
2. 개인정보보호 관리체계를 수립·운영하는 방법과 절차
3. 개인정보보호 관리체계 및 보호대책 구현과 관련되는 문서 목록

④ 신청기관은 인증범위 및 일정 등을 인터넷진흥원 또는 인증기관과 사전 협의하여 신청하여야 한다.

⑤ 인터넷진흥원 또는 인증기관은 인증심사 실시 여부를 판단하기 위하여 제12조에 따른 신청기관의 인증심사 준비 여부를 확인할 수 있으며, 신청기관의 준비가 미흡한 경우에는 신청기관에 이를 보완할 것을 요구할 수 있다.

⑥ 인터넷진흥원 또는 인증기관은 인증범위의 변경이 필요한 경우에 이를 신청기관과 협의하여 변경할 수 있다.

제14조(인증심사 계약의 체결) 신청기관은 인터넷진흥원 또는 인증기관과 협의한 후 심사기간, 심사인원, 인증수수료, 인증범위, 인증 정지 또는 취소 등을 포함하는 인증심사 계약을 체결한다.

제15조(인증수수료의 산정) ① 인증 수수료는 별표 4의 개인정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

② 인터넷진흥원 또는 인증기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 같은 인증대상에 대하여 2개 이상의 신청기관이 있는 경우 또는 하나의 신청기관이 다수의 인증대상에 대하여 인증신청을 한 경우에는 통합하여 심사 일수를 산정하고 그에 따라 수수료를 정할 수 있다.

④ 인터넷진흥원 또는 인증기관은 신청기관의 인증범위가 제16조제2항에 따라 추가 또는 조정된 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

⑤ 신청기관은 최초심사, 사후심사 및 갱신심사 신청시 수수료를 납부하여야 하며, 수수료를 납부하지 않은 경우에 인증심사를 실시하지 아니할 수 있다.

⑥ 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인증기관에 납부하여야 한다.

제5장 인증심사의 기준 및 방법

제16조(인증기준) ① 신청기관의 인증심사 기준은 신청유형별로 별표 5의 구분에 따른다.

② 인터넷진흥원 또는 인증기관은 신청기관과 협의를 통해 개인정보 처리 규모, 업무특성 등을 고려하여 인증심사 항목을 추가 또는 조정할 수 있다.

제17조(인증심사팀 구성) ① 인터넷진흥원 또는 인증기관은 인증심사 계약을 체결한 때에는 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원 또는 인증기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 개인정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제18조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 별표 5의 인증기준에 적합한지에 대하여 개인정보보호 관리체계 구축·운영 관련 개인정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 개인정보보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원 또는 인증기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 30일 이내에 보완조치를 요구할 수 있다.

⑥ 인터넷진흥원 또는 인증기관은 보완조치 결과를 확인하기 위하여 필요한 때에는 현장 확인을 할 수 있다.

제19조(심사중단) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

1. 신청기관이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청기관의 귀책사유로 인하여 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우

2. 신청기관이 제출한 관련 자료 등을 검토한 결과 인증 준비가 되었다고 볼 수 없는 경우

3. 인증심사 후 제18조제4항에 따른 보완조치를 최대 90일(재조치 요구 60일 포함) 이내에 하지 않은 경우

4. 천재지변 및 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우

② 인터넷진흥원 또는 인증기관은 제1항에 따라 인증심사를 중단하는 때에는 그 사유를 신청기관에 서면으로 통보하여야 한다.

③ 인터넷진흥원 또는 인증기관은 제1항의 인증심사 중단 사유가 해소되거나 제29조에 따른 이의제기 처리결과에 따라 인증심사를 재개하거나 종결할 수 있다.

제6장 인증위원회의 구성 및 운영

제20조(인증위원회의 구성) ① 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부

2. 사후심사 결과 제28조제1항에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부

3. 제28조제1항에 따른 인증의 취소에 관한 사항

4. 제29조에 따른 이의신청에 관한 사항

5. 그 밖에 개인정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 1명을 포함한 35인 이내의 위원으로 구성하되, 위원은 개인정보보호 전문가, 변호사, 교수 등 개인정보보호 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

④ 인터넷진흥원 또는 인증기관의 장은 위원이 법령 또는 이 규정을 위반한 때에는 해당 위원을 해촉할 수 있다.

제21조(인증위원회의 운영) ① 인증위원회의 회의는 인터넷진흥원 또는 인증기관의 요구로 개최하되, 회의마다 위원장과 인증위원의 전문분야를 고려하여 5인 이상의 인증위원으로 구성·운영한다.

② 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다. 다만, 긴급한 경우나 부득이한 사유가 있는 경우에는 그러하지 아니하다.

③ 인증위원회 위원장은 제20조제1항의 각호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

④ 인증위원회는 심의를 위하여 필요하다고 인정되는 경우에는 인증심사에 참여한 인증심사원 또는 관련 전문가로부터 그에 관한 의견을 들을 수 있다.

⑤ 그밖에 인증위원회의 운영에 관한 세부사항은 인증위원회의 의결을 거쳐 인터넷진흥원 또는 인증기관의 장이 정한다.

제22조(제척·기피·회피) ① 인증위원회 위원은 신청기관과 다음 각 호의

사항 중 어느 하나에 해당하는 때에는 심의·의결에 관여할 수 없다.

1. 위원 본인과 직접적인 이해관계가 있는 사항
2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
3. 위원이 되기 전에 감사·수사 또는 조사에 관여한 사항

② 위원에게 심의·의결의 공정을 기대하기 어려운 사정이 있는 경우 신청기관은 기피신청을 할 수 있고, 위원회는 의결로 이를 결정한다.

③ 위원은 제척사유 또는 기피사유에 해당하는 경우에는 자기 스스로 심의·의결을 회피할 수 있다.

제7장 인증서의 발급·관리

제23조(인증서의 발급 등) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관에게 결과를 통보하고, 신청기관의 개인정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제8호 서식의 개인정보보호 관리체계 인증서를 발급하여야 한다.

② 제1항에 따른 개인정보보호 관리체계 인증서의 유효기간은 3년으로 한다.

③ 인터넷진흥원 또는 인증기관의 장은 인증서 발급 이외의 건에 대해 인증위원회의 심의·의결 결과를 제출 받은 때에는 신청기관에게 결과를 즉시 통보하여야 한다.

제24조(인증서 관리 및 재발급) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제9호 서식의 개인정보보호 관리체계 인증서 재발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제10호 서식의 개인정보보호 관리체계 인증서

변경 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제25조(인증의 표시 및 홍보) ①「개인정보 보호법」제13조제3호 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」제52조에 따른 인증의 표시는 별표 6과 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 제13조에 따른 인증의 유형과 인증범위 및 유효기간을 함께 표시하여야 한다.

제8장 인증서 사후관리

제26조(사후심사) ① 인증 취득기관은 발급받은 인증서의 유효기간 중 연 1회 이상 인터넷진흥원 또는 인증기관에 사후심사를 신청하여야 한다.

② 사후심사는 제4장 및 제5장을 준용하여 진행한다.

제27조(갱신심사) ① 인증 취득기관은 인증서 유효기간 만료 3개월 전까지 갱신심사를 신청하여야 한다.

② 갱신심사는 제4장, 제5장을 준용하여 진행한다.

③ 인증 취득기관이 제1항에 따른 인증의 갱신을 신청하지 않고 인증의 유효기간이 경과한 때에는 인증의 효력은 상실된다.

제28조(인증의 취소) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 사유를 발견한 때는 인증위원회 심의·의결을 거쳐 인증을 취소할 수 있다.

1. 거짓 혹은 부정한 방법으로 인증을 취득한 경우
2. 제16조제1항에 따른 인증기준에 미달하게 된 경우
3. 인증 취득기관이 제26조제1항에 따른 사후심사 또는 제27조제1항에 따른 갱신심사를 받지 않았거나 제18조제4항에 따른 보완조치를 하지 않은 경우
4. 인증 받은 내용을 홍보하면서 제25조제2항에 따른 인증의 유형과 인증범위 및 유효기간을 허위로 표기하거나 누락한 경우
5. 인증을 취득한 기관이 제26조 및 제27조에 따른 사후관리를 거부 또는 방해하는 경우

② 인터넷진흥원 또는 인증기관은 제1항에 따라 인증을 취소한 경우에 인증 취득기관에 통지하고, 제23조에 따라 발급한 인증서를 회수한다.

제29조(이의신청) ① 신청기관 또는 인증 취득기관이 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날로부터 15일 이내에 인터넷진흥원 또는 인증기관에 이의신청을 할 수 있다.

② 인터넷진흥원 또는 인증기관은 제1항에 따른 이의신청이 이유가 있다고 인정되는 경우에는 인증위원회에 재심의를 요청할 수 있다.

③ 인터넷진흥원 또는 인증기관은 이의신청에 대한 처리결과를 신청기관 또는 인증 취득기관에 서면으로 통지하여야 한다.

제30조(비밀유지 등) ① 인터넷진흥원 또는 인증기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 정당한 권한 없이 또는 허용된 권한을 초과하여 업무상 지득한 비밀에 관한 정보를 누설하거나 이를 업무 목적 이외에 사용하여서는 아니 된다.

② 인터넷진흥원 또는 인증기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 인증에 관련하여 일체의 금전, 금품, 이익 등을 부당하게 수수하여서는 아니 된다.

제31조(인증업무 지침) 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

제32조(재검토 기한) 행정자치부 및 방송통신위원회는「행정규제기본법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2016년 1월 1일을 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

제1조(시행일) 이 고시는 2016년 1월 1일부터 시행한다.

제2조(인증심사원 및 인증 취득기관에 관한 경과조치) ① 이 고시 시행 이

전에 「개인정보 보호 인증제 운영에 관한 규정」(행정자치부고시 제2014-1호) 제23조 또는 「개인정보보호 관리체계 인증 등에 관한 고시」(방송통신위원회고시 제2013-17호) 제9조의 인증심사원 자격요건에 상응하는 요건을 갖추고 인터넷진흥원, 한국정보화진흥원으로부터 심사원으로 위촉된 자는 이 고시에 의한 인증심사원 자격을 취득한 것으로 본다.

② 이 고시 시행 이전에 「개인정보 보호 인증제 운영에 관한 규정」(행정자치부고시 제2014-1호) 제17조 또는 「개인정보보호 관리체계 인증 등에 관한 고시」(방송통신위원회고시 제2013-17호) 제22조에 따른 인증서를 발급받은 자는 인터넷진흥원 또는 인증기관으로부터 이 고시에 의한 인증서를 발급받은 것으로 본다.

③ 신청기관 또는 이 고시의 시행 이전에 인증을 취득한 자는 이 고시의 시행으로부터 1년간 제16조에 따른 인증기준 대신 「개인정보 보호 인증제 운영에 관한 규정」(행정자치부고시 제2014-1호) 제9조 또는 「개인정보보호 관리체계 인증 등에 관한 고시」(방송통신위원회고시 제2013-17호) 제17조에 따른 인증 기준으로 심사를 신청할 수 있다. 이 경우, 인터넷진흥원 또는 인증기관은 신청받은 인증기준으로 심사를 수행할 수 있다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제3항 관련)

구 분	제 출 서 류
1. 개인정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 별지 제4호 서식에 따른 개인정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 부채비율 및 자기자본 이익률의 계산내역 (회계결산내역 등 관련 증빙자료) 나. 인증심사 업무 운영체계 관련 규정 및 지침 등 o 심사기관의 운영체계 및 인증의 품질관리 o 인증심사 업무를 수행하는 직원에 대한 운영관리 등의 내부규정 o 인증심사 업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가 항목	세부 평가기준
1. 인증심사원 5명이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 선임심사원 1명 이상 확보해야 함
2. 인증기관 공정성 확보 여부	o 개인정보보호 관리체계 인증기관으로 지정을 받으려는 기관은 인증업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="4">1.조직내 직원들의 개인정보보호 전문성
(30)</td><td rowspan="3">개인정보보호 업무 전문성</td><td>10</td><td>비율</td><td>o 심사원 이상 인력 수
<table><tr><td>심사원 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 χ%</td></tr><tr><td colspan="2">※ χ = (심사원 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o (개인)정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><td>박사학위소지자·
기술사 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 χ%</td></tr><tr><td colspan="2">※ χ = (박사학위 소지자·기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><td>자격증 소지자 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 χ%</td></tr><tr><td colspan="2">※ χ = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>개인정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 개인정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><td>총 참여 일수(단위 : 일)</td><td>점수</td></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 χ%</td></tr><tr><td colspan="2">※ χ = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><td>2. 시설(10)</td><td>사무공간 · 인증심사 서류 보관 장소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 장소</td><td>2점</td></tr>
<tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안시설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3.신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율(부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50%미만</td><td>5점</td></tr>
<tr><td>50%이상 ~ 100%미만</td><td>4점</td></tr>
<tr><td>100%이상 ~ 150%미만</td><td>3점</td></tr>
<tr><td>150%이상 ~ 200%미만</td><td>2점</td></tr>
<tr><td>200%이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률(당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20%이상</td><td>5점</td></tr>
<tr><td>20%미만 ~ 15%이상</td><td>4점</td></tr>
<tr><td>15%미만 ~ 10%이상</td><td>3점</td></tr>
<tr><td>10%미만 ~ 5%이상</td><td>2점</td></tr>
<tr><td>5%미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="4">4. 인 증 업 무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증 품질 관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보증 방안</td><td>5점</td></tr>
<tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>o 인증의 품질 보증 및 관리방안</td><td>5점</td></tr>
<tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인 증 업 무 를 수 행 하 는 직 원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증 업무를 수행하는 직원에 대한 규정 보유 및 동 규정의 타당성과 실효성
- 인증 업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증 업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>o 인증 업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성과 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>5</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증 업무 수행 방법, 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증 수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 지원체계</td><td>15</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도·해산 등에 따른 신청기관 피해 보상 관련 대책마련 여부</td><td>5점</td></tr>
<tr><td>o 인증의 품질 제고를 위한 지원방안</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td rowspan="3">5. 가점 및 감점</td><td>인증심사업무를 전담하는 인증심사원 보유수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table><tr><th>구분</th><th>점수</th></tr><tr><td>10명 이상</td><td>5점</td></tr><tr><td>10명 미만 ~ 5명 이상</td><td>배점의 χ%</td></tr><tr><td>5명 미만</td><td>없음</td></tr><tr><td colspan="2">※ χ = (인원수/10명) × 100</td></tr></table></td></tr>
<tr><td>개인정보보호 관리체계 인증의 취득 및 유지</td><td>2
(가점)</td><td>인증 취득 및 유지</td><td>o 개인정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td>자격취소 사실</td><td>5
(가점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 행정자치부 및 방송통신위원회가 부여한 (개인)정보보호 관련 수행 자격이 취소된 경우
- (개인)정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. ‘시설’, ‘인증업무 운영체계’에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 3]

인증심사원 자격 요건(제7조 관련)

1. 인증심사원 자격 신청 요건

□ 기본요건

4년제 대학졸업 이상 또는 이와 동등학력을 취득한 자로서 정보기술 유관경력 또는 정보보호 유관경력을 합하여 6년 이상의 경력을 보유하고 이 중 개인정보보호 실무경력 2년 이상을 보유

가. “동등학력”이란 고등학교 졸업자는 4년 이상, 2년제 대학 졸업자는 2년 이상 업무경력을 말한다.

나. “정보기술 유관경력”이란 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 정보기술 관련 법률자문 경력을 말한다.

다. “정보보호 유관경력”이란 공공기관, 기업체, 교육・연구기관에서 정보보호를 위한 공통기반기술(암호기술, 인증기술 등) 분야, 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등) 분야, 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등) 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등의 업무를 수행한 경력 또는 정보보호 관련 법률자문 경력을 말한다.

라. “개인정보보호 실무경력”이란 공공기관・기업체 등에서 개인정보보호 업무 수행, 개인정보보호 컨설팅, 개인정보보호 관련 법률자문 등의 업무를 수행한 경력을 말한다.

마. 변호사법에 따른 변호사의 경우에는 6년의 정보기술 유관경력 또는 정보보호 유관경력을 보유한 것으로 본다.

바. 모든 해당 경력은 신청일 기준 최근 10년 이내의 경력에 한해 인정하며 최근 5년 이내에 2년 이상의 관련 경력이 포함되어야 한다.

□ 경력 대체 요건

구 분	경력 인정요건 해당 자격	인정기간
정보보호 또는 정보기술 유관경력 인정 요건 (중복경력인정불가)	가. "정보보호" 또는 "정보기술" 관련 박사학위 취득자 나. 국가기술자격법시행규칙 별표2의 '정보기술' 직무분야 기술사 다. 정보시스템감리사(ISA)	2년
	가. "정보보호" 또는 "정보기술" 관련 석사학위 취득자 나. 국가기술자격법시행규칙 별표2의 '정보기술' 직무분야 기사 다. 정보보안기사(정보보호전문가) 라. 국제공인정보시스템감사사(CISA) 마. 국제공인정보시스템보안전문가(CISSP)	1년
개인정보보호 실무경력 인정 요건 (중복경력인정불가)	가. "개인정보 보호" 관련 박사학위 취득자	2년
	가. "개인정보 보호" 관련 석사학위 취득자 나. 개인정보보호 관리사(CPPG)	1년

2. 인증심사원 등급별 자격 요건

구 분	자격 기준
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 시행하는 인증심사원 양성교육 과정을 수료하고 평가에 합격한 자
심사원	o 심사원보 자격 취득자로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임 심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

[별표 4]

개인정보보호 관리체계 인증 수수료 산정기준(제15조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가산정 가이드의 정보보안 컨설팅비를 준용한다.

인증심사원 등급	컨설턴트 등급
선임심사원	전임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사 업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 5]

개인정보보호 관리체계 인증기준(제16조 관련)

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
개인정보보호 관리과정	1.관리체계 수립(7)	1.1	정책 및 범위	1.1.1	정책의 수립	개인정보보호정책과 시행문서를 수립하여 조직의 개인정보보호 방침과 방향을 명확하게 제시하여야 한다. 또한, 개인정보보호(관리)책임자 등 경영진의 승인을 받고 임직원 및 관련자에게 공표하여야 한다.	○	○	○	○
				1.1.2	정책의 유지관리	개인정보보호정책 및 시행문서는 관련 법·규제를 준수하고, 상위 정책과 일관성을 유지하여야 한다. 또한, 정기적으로 검토하여 필요한 경우 제·개정 및 이력관리하고 운영기록을 생성·유지하여야 한다.	○	○	○	
				1.1.3	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함하는 개인정보보호 관리체계 범위를 설정하여야 한다.	○	○	○	
		1.2	경영진의 책임	1.2.1	경영진의 참여	개인정보보호 관리체계 수립 및 운영 등 조직이 수행하는 개인정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.	○	○		
		1.3	조직	1.3.1	개인정보보호(관리)책임자의 지정	지속적인 개인정보보호 관리체계 운영활동을 위하여 개인정보보호(관리)책임자를 지정하여야 한다.	○	○	○	○
				1.3.2	조직의 구성	조직 전반의 중요한 개인정보보호 관련사항을 검토 및 의사결정할 수 있는 조직(협의체)을 구성하여야 한다. 또한 개인정보보호 관리체계 운영활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.	○	○	○	
				1.3.3	역할 및 책임	개인정보관리(보호)책임자 및 개인정보를 취급하는 각 부서의 책임자, 담당자에 대한 역할과 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다. 또한, 상호 의사소통할 수 있는 보고체계를 정의하여야 한다.	○	○	○	

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
	2.실행 및 운영(5)	2.1	개인정보 식별	2.1.1	개인정보 식별	조직의 개인정보 및 개인정보 관련 자산을 식별하고 중요도를 결정하여 보안등급을 부여한 후 그에 따른 취급절차를 정의·이행하여야 한다. 또한, 자산별 책임 소재를 명확히 정의하여야 한다.	○	○	○	○
				2.1.2	개인정보 흐름 파악	조직의 개인정보 관련 서비스 및 업무에서 개인정보 흐름을 파악하여 개인정보 흐름도(표)를 작성하고 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	○	○	○	
		2.2	위험 관리	2.2.1	위험관리 방법 및 계획 수립	조직의 개인정보보호 전 영역에 대하여 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리계획을 수립하여야 한다.	○	○	○	
				2.2.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.	○	○	○	
				2.2.3	이행계획 수립 및 보호대책 구현	위험을 수용 가능한 수준으로 감소시키기 위해 개인정보보호대책을 선정하고 이행계획을 수립하여 경영진의 승인을 받아야 한다. 또한, 수립된 이행계획에 따라 보호대책을 구현하여야 한다.	○	○	○	
	3.검토 및 모니터링(2)	3.1	개인정보 보호체계의 검토	3.1.1	법적요구사항 준수검토	조직이 준수해야 할 개인정보보호 관련 법적 요구 사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.	○	○	○	
				3.1.2	내부 감사	개인정보보호 관리체계가 효과적으로 운영되고 있는지를 점검하기 위해 연 1회 이상 내부감사 계획을 수립하고 수행하여야 한다. 내부감사를 통해 발견된 문제점을 보완하여 경영진에게 보고하여야 한다.	○	○	○	

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
	4.교정 및 개선 (2)	4.1	교정 및 개선 활동	4.1.1	개인정보 보호 개선 활동	주기적 또는 상시적으로 수행해야 하는 개인정보 보호 활동을 문서화하여 그 운영현황을 지속적으로 점검·개선하는 등의 관리를 하여야 한다.	○	○	○	
		4.2	내부 공유 및 교육	4.2.1	내부 공유 및 교육	개인정보 관리계획을 운영 또는 이행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.	○	○	○	○
생명주기 및 권리 보장	5.개인정보 생명주기 관리 (16)	5.1	개인정보 수집 시 보호조치	5.1.1	개인정보 수집 제한	서비스 제공을 위해 필요한 최소한의 정보만을 수집해야 한다. 개인정보 수집 시 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	○	○	○	○
				5.1.2	정보주체의 동의	개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체(이용자)의 동의를 얻은 후에 수집해야 한다.	○	○	○	○
				5.1.3	법정대리인 동의 및 고지	만14세 미만 아동의 개인정보를 수집할 경우 법정대리인에게 필요한 사항을 고지하고, 동의를 획득하여야 한다.	○	○	○	○
				5.1.4	민감정보 및 고유식별정보의 수집 제한	고유식별정보와 민감정보는 정보주체(이용자)의 별도 동의를 받거나 다른 법령에서 처리를 요구하여 허용된 경우를 제외하고는 수집할 수 없다.	○	○	○	○
				5.1.5	주민등록번호 수집·이용 제한	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우를 제외하고 주민등록번호를 수집·이용할 수 없다.	○	○	○	○
				5.1.6	주민등록번호 대체수단	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우에도 주민등록번호 대체수단을 제공해야 한다.	○	○	○	○
				5.1.7	간접수집 보호조치	시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집 개인정보에 대하여 적절한 보호대책을 수립·이행해야 한다.	○	○	○	○
				5.1.8	개인정보 처리(취급)방침	개인정보처리(취급)방침을 수립하여 정보주체(이용자)가 언제든지 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
		5.2	개인정보 이용 및 제공	5.2.1	개인정보 제3자 제공	개인정보를 제3자에게 제공 시, 관련내용을 고지하고 동의를 획득한 후 제공하여야 하며, 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제해야 한다.	○	○	○	○
				5.2.2	제공받은 개인정보의 관리	개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않고 제3자에게 제공하지 않아야 하며, 개인정보를 안전하게 관리하여야 한다.	○	○	○	○
				5.2.3	개인정보 목적 외 이용 및 제공	개인정보를 정보주체(이용자)에게 고지·동의받은 범위에서 벗어나지 않도록 이용하여야 하며, 만약 동의 범위를 벗어날 경우 정보주체(이용자)로부터 추가 동의를 획득하고, 적절한 보호조치를 하여야 한다.	○	○	○	○
				5.2.4	개인정보의 이전	영업의 양도, 합병 등으로 개인정보를 이전하는 경우 적절한 보호대책을 수립·이행해야 한다. 또한, 개인정보를 해외로 이전하는 경우 개인정보에 대한 적절한 보호대책을 수립·이행해야 한다.	○	○	○	○
		5.3	개인정보 보유 시 보호조치	5.3.1	개인정보 품질 보장	수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성, 완전성, 최신성을 유지 하여야 한다.	○	○	○	○
				5.3.2	개인정보 파일관리	개인정보파일을 운용하는 공공기관은 그 현황을 행정자치부에 등록하여야 하고, 변경사항 발생 시, 이를 고지하여야 한다.	○			
		5.4	개인정보 파기 시 보호조치	5.4.1	개인정보 파기 규정 및 절차	개인정보의 보유기간 및 파기와 관련한 내부 규정을 수립하고, 파기 관련 보호조치를 마련하여야 한다. 또한, 개인정보 수집 동의 등에 대한 기록은 탈퇴 전까지 안전하게 보관하여야 한다.	○	○	○	○
				5.4.2	개인정보의 파기	개인정보의 수집 목적이 달성된 경우, 안전한 방법으로 지체없이 파기하고 관련 사항은 기록 관리하여야 한다. 개인정보의 수집목적 달성 후에도 관련 법령 등에 의해 보유가 필요하다면 정보주체(이용자)에게 고지하고 최소한의 항목을 보유해야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
	6.정보주체 권리 보장 (4)	6.1	권리보장	6.1.1	개인정보 열람	개인정보에 대한 열람·정정·삭제 방법 및 절차를 제공하고, 정보주체(이용자)가 요구 시 열람하게 하여야 한다.	○	○	○	○
				6.1.2	개인정보 정정·삭제	정보주체(이용자)가 개인정보에 대한 정정·삭제 요구 시 지체없이 처리하고, 기록을 남겨야 한다. 또한, 개인정보 이용내역을 법령에 따라 주기적으로 통지하여야 한다.	○	○	○	○
				6.1.3	개인정보 처리 정지	정보주체(이용자)에게 개인정보에 대한 처리정지 방법 및 절차를 제공하고, 처리정지 요구 시 지체없이 처리하고, 기록을 남겨야 한다.	○	○	○	○
				6.1.4	권리행사의 방법 및 절차	정보주체(이용자)가 열람 등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 상담창구 등 필요한 절차를 마련하여야 한다.	○	○	○	○
개인정보 보호대책	7.관리적 보호조치 (10)	7.1	교육 및 훈련	7.1.1	교육 및 훈련 시행·평가	연간 개인정보보호 교육 계획을 수립하고, 관련 임직원 및 외부자를 대상으로 주기적인 교육을 시행하여야 한다. 또한, 교육 시행에 대한 기록을 남기고 결과를 평가하여 다음 교육에 반영하여야 한다.	○	○	○	○
		7.2	개인정보 취급자 관리	7.2.1	개인정보 취급자 감독	개인정보를 취급하는 임직원 및 외부자를 최소한으로 제한하고 개인정보취급자 목록을 관리하여야 한다. 또한 개인정보보호 책임의 충실한 이행 여부에 대해 상벌 규정을 마련하여야 한다.	○	○	○	○
				7.2.2	보안 서약서	개인정보를 취급하는 개인정보취급자, 임시직원, 외부자 등에게 보안서약서를 받아야 한다.	○	○	○	○
				7.2.3	퇴직 및 직무변경 관리	개인정보취급자의 퇴직 및 직무변경 시 자산반납, 계정 및 권한 회수.조정, 결과 확인 등의 개인정보취급자 인사 관리 절차를 수립하고 이행하여야 한다.	○	○	○	○
		7.3	위탁업무 관리	7.3.1	외부 위탁 계약	개인정보 처리업무를 외부에 위탁하는 경우 개인정보보호에 관한 요구사항, 관리감독, 법규정 위반의 배상책임 등에 관한 사항을 계약서 등에 문서화하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
				7.3.2	정보주체 고지	개인정보 처리업무 위탁시 수탁자, 수탁목적 등 관련사항을 정보주체(이용자)에게 고지하고 필요한 경우 동의를 받아야 한다.	○	○	○	○
				7.3.3	위탁자 관리·감독	위탁 업체가 계약서 및 서비스 수준 협약, 관련 법·규정 등에 명시된 사항을 충분히 이행하는지 주기적으로 관리·감독해야 한다.	○	○	○	○
		7.4	침해사고 관리	7.4.1	침해사고 대응절차 및 체계구축	개인정보 침해사고 대응절차를 수립하고, 개인정보 침해사고 대응이 신속하게 이루어질 수 있도록 대응체계를 구축하며 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.	○	○	○	
				7.4.2	침해사고 훈련 및 개선	침해사고 대응절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다. 모의훈련 결과는 침해사고 대응절차에 반영하여 주기적으로 개선하여야 한다.	○	○	○	
				7.4.3	침해사고 대응	개인정보 침해사고 발생 시 절차에 따라 신속히 복구를 수행하고, 사고분석 후 발견된 취약점은 관련 조직 및 임직원과 공유하며, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여 침해사고 대응체계에 반영하여야 한다.	○	○	○	
	8.기술적 보호조치 (32)	8.1	접근권한 관리	8.1.1	접근통제 정책 수립	개인정보보호 요구사항을 기반으로 비인가자의 접근을 통제할 수 있도록 개인정보취급자의 접근통제 정책을 수립하여야 한다.	○	○		
				8.1.2	개인정보 취급자 등록	개인정보 및 개인정보처리시스템의 접근을 통제하기 위한 개인정보취급자 등록 및 해지 절차를 마련하여야 한다. 또한, 개인정보 취급 PC의 보안책임이 자신에게 있음을 규정화하고 인식시켜야 한다.	○	○	○	○
				8.1.3	개인정보 취급자 권한관리	개인정보처리시스템의 접근권한은 최소한의 업무 수행자에게만 부여하고 권한변경 내역을 보관하여야 한다.	○	○	○	○
				8.1.4	특수권한 관리	개인정보 및 개인정보처리시스템에 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
				8.1.5	개인정보 취급자 접근 권한 검토	개인정보 및 개인정보처리시스템 등을 사용하는 개인정보취급자의 접근권한 현황을 정기적으로 점검해야 한다.	○	○	○	
				8.1.6	개인정보 취급자 인증 및 식별	개인정보처리시스템 접근 시 안전한 인증 절차에 따라 통제하고, 필요한 경우 법적요구사항 등을 고려하여 강화된 인증방식을 적용해야 한다.	○	○	○	○
				8.1.7	비밀번호 관리	법적요구사항, 외부 위협요인 등을 고려하여 개인정보취급자 및 사용자, 정보주체(이용자)의 비밀번호 관리절차를 수립하고 이행하여야 한다.	○	○	○	○
		8.2	접속기록 관리	8.2.1	개인정보처리시스템 접속기록 관리	개인정보처리시스템의 접속기록을 보관하고, 접속기록의 정확성을 보장하기 위해 관련 장비 및 시스템을 표준시간으로 동기화하여 해야 한다.	○	○	○	○
				8.2.2	접속기록 모니터링	접속기록은 위·변조되지 않도록 보호대책을 적용하여야 하며, 개인정보의 오남용이 발생되지 않도록 모니터링을 수행하여야 한다. 또한 문제 발생 시 적절한 사후조치가 적시에 이루어져야 한다.	○	○	○	
		8.3	접근통제 영역관리	8.3.1	네트워크 접근	유·무선 네트워크에 대한 비인가 접근을 통제하기 위해 네트워크 접근통제 관리절차를 수립하고 서비스, 사용자 그룹, 개인정보 자산의 중요도, 법적요구사항에 따라 네트워크를 분리하여야 한다.	○	○	○	○
				8.3.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.	○	○	○	○
				8.3.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 개인정보를 취급하는 응용프로그램 접근권한을 제한하여야 한다.	○	○	○	○
				8.3.4	데이터 베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립·이행하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
				8.3.5	원격 운영접근	내부 네트워크를 통하여 개인정보처리시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 외부 네트워크를 통하여 개인정보처리시스템을 관리하는 것은 원칙적으로 금지한다. 부득이한 사유로 인해 허용하는 경우에는 관련 법률에 따른 보호대책을 수립하여야 한다.	○	○	○	
				8.3.6	인터넷 접속 통제	개인정보처리시스템에 접근 가능한 개인정보취급자의 PC는 인터넷 접속 또는 서비스를 제한 및 통제하고, 필요시 인터넷 접속내역을 모니터링 하여야 한다.	○	○	○	
		8.4	운영보안	8.4.1	운영절차 수립	개인정보처리시스템 동작에 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.	○	○		
				8.4.2	직무분리	개인정보처리시스템의 오남용 예방을 위해 직무 분리 기준을 수립·적용하고, 직무 분리가 어려운 특수한 경우 별도의 보호대책을 마련하여야 한다.	○	○		
				8.4.3	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템과 개인정보취급자 단말기(PC, 노트북 등)를 보호하기 위해 보호대책을 수립하여야 한다.	○	○	○	○
				8.4.4	취약점 점검	개인정보처리시스템에 대한 비인가 접근 시도 등을 예방하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.	○	○	○	
				8.4.5	개인정보 표시제한	개인정보 조회, 출력 등을 수행할 경우, 마스킹 기술 등을 통해 개인정보 표시를 제한하여야 한다.	○	○	○	
				8.4.6	보안 시스템 설치·운용	불법적인 접근 및 침해사고 방지를 위해 침입차단 및 탐지 기능을 포함한 시스템을 설치·운용하여야 한다. 또한, 보안시스템 운영절차를 수립하고 보안시스템별 정책적용 현황을 관리하여야 한다.	○	○	○	
				8.4.7	공개 서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
				8.4.8	모바일 기기 관리	업무 목적으로 모바일기기를 내·외부 네트워크에 연결하여 사용할 경우 모바일기기 접근통제 대책을 수립하여야 한다.	○	○	○	
				8.4.9	백업 관리	데이터의 무결성 및 개인정보처리시스템의 가용성을 유지하기 위해 백업 절차를 수립하여 주기적으로 백업 및 관리를 하여야 한다.	○	○		
				8.4.10	패치 관리	소프트웨어, 운영체제, 보안시스템 등에 대하여 시스템에 미치는 영향을 분석하여 주기적으로 최신 패치를 적용하여야 한다.	○	○	○	○
		8.5	암호화 통제	8.5.1	암호화 정책 수립	개인정보를 안전하게 관리하기 위하여 법적 요구사항을 반영한 암호화 정책을 수립하여야 한다.	○	○	○	
				8.5.2	암호화 적용	암호화 정책에 따라 개인정보 저장 및 전송, 원격접속 시 암호화를 수행하고 암호키를 안전하게 관리하여야 한다.	○	○	○	○
		8.6	개발 보안	8.6.1	개인정보 영향평가	개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 수행하여야 한다.	○			
				8.6.2	개발 시 보안조치	개인정보처리시스템을 개발·변경 시 개인정보 영향평가 수행 결과를 보안 요구사항에 포함하여 개발하고, 안전한 코딩방법에 따라 구현 및 시험을 수행하며, 취약성에 대한 노출여부를 점검하여 이에 대한 보호대책을 수립하여야 한다.	○	○		
				8.5.3	개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템과 원칙적으로 분리하고, 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하며, 실행코드는 시험과 인수 절차에 따라 실행되어야 한다.	○	○		
				8.5.4	시험 데이터 및 소스 프로그램 보안	운영데이터를 테스트 데이터로 사용할 시 보호조치에 관한 절차를 수립·이행하여야 한다. 또한, 소스 프로그램은 인가된 사용자만이 접근하도록 통제하고 운영환경에 보관하지 않아야 한다.	○	○		

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
				8.5.5	외주개발 보안	개인정보처리시스템의 개발을 외주 위탁하는 경우 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.	○	○		
	9.물리적 보호조치 (8)	9.1	영상정보처리기기 관리	9.1.1	영상정보처리기기의 설치·운영 제한	영상정보처리기기 설치·운영 시, 설치 목적에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호조치를 마련하여야 한다.	○	○	○	○
				9.1.2	영상정보처리기기 설치·운영 사무의 위탁 관리	영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 적절한 위탁절차를 마련하여야 한다.	○			
		9.2	물리적 보안관리	9.2.1	보호구역의 지정 및 관리	주요 설비 및 시스템을 보호하기 위하여 보호구역을 지정하고 보호구역 내의 작업 절차를 포함하여 보호대책을 수립·이행하여야 한다. 보호구역의 특성에 따라 보호설비를 갖추고 운영하여야 한다. 또한 외부 집적정보통신시설에 위탁·운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토하여야 한다.	○	○	○	
				9.2.2	출입통제 및 사무실 보안	보호구역은 인가된 사람만이 접근할 수 있도록 통제하고 출입 및 접근 이력을 주기적으로 검토하여야 한다. 또한 사무실에서 공용으로 사용하는 사무용 기기 등에서 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.	○	○	○	○
				9.2.3	개인 업무 환경 보안	책상 위에 중요 문서나 저장매체를 남겨놓지 않고, 중요정보가 노출되지 않도록 보호대책을 수립·이행하여야 한다.	○	○	○	○

인증기준						상세내용	적용 유형			
							유형(4) 공공기관	유형(3) 대기업	유형(2) 중소기업	유형(1) 소상공인
		9.3	매체 관리	9.3.1	개인정보처리시스템 저장매체 관리	개인정보처리시스템 저장매체 관리절차를 수립하여 운영하고, 개인정보처리시스템 폐기 및 재사용 시 매체에 기록된 개인정보는 복구 불가능하도록 완전히 삭제하여야 한다.	○	○	○	
				9.3.2	휴대용 저장매체 관리	휴대용 저장매체를 통해 개인정보 유출이 발생하거나 악성코드가 감염되지 않도록 관리하고, 개인정보가 포함된 휴대용 저장매체는 안전한 장소에 보관하여야 한다.	○	○	○	
				9.3.3	이동컴퓨팅관리	보호구역 내 임직원 및 외부자의 이동컴퓨팅에 대하여 반·출입을 통제하고 기록·관리하여야 한다.	○	○	○	

[별표 6]

개인정보보호 관리체계 인증의 표시(제25조 관련)

1. 도안모형

인증유형 :

유효기간 :

인증범위 :

2. 인증 표시에 대한 유의사항

가. 개인정보보호 관리체계 인증 취득 사실의 홍보는 개인정보보호 관리체계 인증서를 발급받은 날부터 효력이 유지되는 동안에만 사용이 가능하다. 인증이 취소된 경우에는 인증에 대한 홍보, 개인정보보호 관리체계 인증서 사용을 중지하여야 한다.

나. 인증 표시를 사용하는 경우 인증유형, 유효기간, 인증범위를 함께 표시하여야 한다.

다. 인증유형을 기재할 때에는 제13조제1항의 신청기관 유형 중 인증받은 기관에 해당되는 유형을 기재하여야 한다.

라. 인증을 취득한 자는 인증의 사실을 과장되거나 불명확한 표현을 사용하여 광고할 수 없다.

3. 인증 표시의 사용 방법

가. 인증 표시는 지정된 색상으로 사용할 수 있다. 또한 색상이 명확하게 나타날 수 있는 바탕색 위에 흑백으로 사용하거나 표시된 인쇄물의 주된 단일색상으로 사용 할 수 있다.

나. 인증 표시의 크기는 표시물 대상의 크기나 표시장소의 여건에 따라 조정할 수 있으며, 같은 비율로 축소 또는 확대하여 표시할 수 있다.

다. 일반문서, 편지의 상단, 송장, 홍보 책자 등에 개인정보보호 관리체계 인증 취득 사실의 내용을 홍보할 수 있다.

4. 인증명판 제작 시 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다.

다. 도안 모형은 인증의 표지를 중앙에 둔다.

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다.

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호 서식] <개정 2016.1.1>

개인정보보호 관리체계 인증기관 지정 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월 이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	□ 신규	□ 재지정	
인증에 관한 업무범위			

「개인정보 보호법」 제13조제3호 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3 및 동법 시행령 제53조의2에 따라 위와 같이 개인정보보호 관리체계 인증기관 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

행정자치부 또는 방송통신위원회 귀중

신청(신고)인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제2호 서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관		처 리 기 관		처 리 기 관		처 리 기 관

210㎜×297㎜[백상지(80g/㎡)]

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호 서식] <개정 2016.1.1>

인증심사원 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증심사원 자격 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신 유관경력 또는 정보보호 유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210㎜×297㎜[백상지(80g/㎡)]

인증심사 업무를 전담하는 직원의 보유현황 (제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

210㎜×297㎜[백상지(80g/㎡)]

개인정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「개인정보 보호법」 제13조제3호 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3 및 동법 시행령 제53조의2에 따라 위와 같이 개인정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

행정자치부 장관 직인

방송통신위원회 위원장 직인

CERTIFICATE OF DESIGNATION
AS
PIMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification WORK :

This is to certify that the above mentioned organization is designated Personal Information Management System (PIMS) Certification Authority in accordance with Article 13 3 of 「Personal Information Protection Act」, Article 47-3 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by
Minister of the Interior
Chairman of Korea Communications Commission

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호 서식] <개정 2016.1.1>

인증실적 보고서

개인정보보호 관리체계 인증기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	개인정보보호 관리체계 인증심사 실적 총계	최초심사	등 건
		사후심사	등 건
		갱신심사	등 건

일련 번호	인증 번호	대상기관(기업)명	인증범위	유효기간	구분		
					최초 심사	사후 심사	갱신 심사

년 월 일

신청인(대표자) (서명 또는 인)

행정자치부 또는
방송통신위원회 귀중

제출서류	1.상세 인증실적 보고서 1부.	

210㎜×297㎜[백상지(80g/㎡)]

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호 서식] <개정 2016.1.1>

개인정보보호 관리체계 인증심사원 자격 신청서

<table>
<tr><td rowspan="5">신청자
인적사항</td><td>성 명</td><td colspan="2"></td><td>생년월일</td><td></td><td rowspan="4">사진</td></tr>
<tr><td>소 속</td><td colspan="5"></td></tr>
<tr><td>주 소</td><td colspan="5">(우:)</td></tr>
<tr><td>휴대전화</td><td colspan="5"></td></tr>
<tr><td>이메일</td><td colspan="6"></td></tr>
<tr><td colspan="2">신청분야</td><td colspan="6"></td></tr>
<tr><td>학력사항</td><td>최종학력</td><td colspan="6">□ 고졸 □ 전문대졸 □ 대졸 □ 석사 □ 박사</td></tr>
<tr><td rowspan="3">경력사항
※ 서류로 증명 가능한 내용만 기술</td><td rowspan="2">총 경력</td><td colspan="2" rowspan="2">총 년 개월
(①+②)
※중복경력은 인정되지 않음</td><td>①정보보호 또는 정보기술 유관경력</td><td colspan="2">총 년 개월
(대체 경력 : 년 포함)</td></tr>
<tr><td>②개인정보보호 유관 경력</td><td colspan="2">총 년 개월
(대체 경력 : 년 포함)</td></tr>
<tr><td>경력대체 내역</td><td colspan="2">□ 정보보호 또는 정보기술 경력 대체사항</td><td colspan="3"></td></tr>
<tr><td></td><td colspan="2">□ 개인정보보호 경력 대체사항</td><td colspan="3"></td></tr>
</table>

개인정보보호 관리체계 인증심사원 자격을 신청하기 위하여 이 신청서를 제출합니다. 본 신청서에 적힌 내용이 사실과 다르거나, 「개인정보보호 관리체계 인증 등에 관한 고시」 별표3에 따른 인증심사원 자격 요건에 해당하지 아니할 때에는 합격 또는 자격을 취소하여도 아무런 이의를 제기하지 않겠습니다.

년 월 일

신청자 (서명 또는 인)

한국인터넷진흥원 귀중

신청인 제출서류	1. 인증심사원 자격 신청 내역서 2. 지격 증빙서류 ①학위증명서 ②관련 경력사항이 구체적으로 기재된 상세 경력증명서 또는 상세 재직증명서 ③기술실적증명서(해당 시) ④자격 증명서(해당 시) 3. 정보보호 서약서 4. 개인정보이용 동의서 등

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호 서식] <개정 2016.1.1>

인증심사원 자격 증명서

발급번호 :

성 명 :

생년월일 : 년 월 일

취득자격 :

유효기간 : . . ~ . .

위 사람은 「개인정보보호 관리체계 인증 등에 관한 고시」 제9조에 따른 개인정보보호 관리체계 인증심사원임을 증명합니다.

년 월 일

한국인터넷진흥원장 직인

210㎜×297㎜[백상지(120g/㎡)]

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호 서식] <개정 2016.1.1>

개인정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ] 최초심사 [ ] 사후심사 [ ] 갱신심사
신청기관 유형	□「소상공인 보호 및 지원에 관한 법률」제2조제1호 및 제2호에 따른 소상공인에 해당하는 사업자 및 그 밖의 사업자 □「중소기업기본법」제2조에 따른 중소기업에 해당하는 사업자 □「대·중소기업 상생협력 촉진에 관한 법률」제2조제2호에 따른 대기업에 해당하는 사업자 및「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제2호에 따른 정보통신서비스 제공자 □「개인정보 보호법」제2조제6호에 따른 공공기관
개인정보보호 관리체계의 범위	
개인정보보호 관리체계의 범위에 포함되어 있는 인원의 수	
개인정보보호 관리체계의 범위에 포함되어 있는 시스템의 수	

「개인정보 보호법」 제13조제3호에 따라 위와 같이 개인정보보호 관리체계의 인증을 신청합니다. 또는,
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3 제1항 및 동법 시행령 제47조에 따라 위와 같이 개인정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는

귀중

개인정보보호 관리체계 인증기관명)

신청(신고)인 제출서류	개인정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210㎜×297㎜[백상지(80g/㎡)]

개인정보보호 관리체계(PIMS) 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증 유형 :

인증의 범위 :

유효기간 :

「개인정보 보호법」 제13조제3호에 따라 위와 같이 개인정보보호 관리체계를 인증합니다. 또는,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의3 제1항 및 동법 시행령 제47조에 따라 위와 같이 개인정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 개인정보보호
관리체계 인증기관 장

직인

CERTIFICATE
OF
Personal Information Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Certification Type :

Scope of Certification :

Period of Validity :

This is to certify that the above mentioned organization is compliant to the assessment standard for Personal Information Management System certification in accordance with Article 13 3 of 「Personal Information Protection Act」 또는, This is to certify that the above mentioned organization is compliant to the assessment standard for Personal Information Management System certification in accordance with Article 47-3 Paragraph 1 of 「Act on Information Network Utilization and Data Protection, etc.」and Article 47 of the Enforcement Decree of the Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency 또는, certification body

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호 서식] <개정 2016.1.1>

개인정보보호 관리체계 인증서 재발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

재발급 사유	

위와 같이 개인정보보호 관리체계 인증서의 재발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는 개인정보보호 관리체계 인증기관명) 귀중

제출서류	해당없음	수수료 없 음

210㎜×297㎜[백상지(80g/㎡)]

■「개인정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호 서식] <개정 2016.1.1>

개인정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 개인정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는 개인정보보호 관리체계 인증기관명) 귀중

제출서류	해당없음	수수료 없 음

210㎜×297㎜[백상지(80g/㎡)]

개인정보보호 자율규제단체 지정 등에 관한 규정

제정 2016. 8. 9. 행정자치부 고시 제2016-31호

제1장 총 칙

제1조(목적) 이 규정은 「개인정보 보호법(이하 "법"이라 한다)」제5조 제3항, 제13조제2호, 제4호 및 제5호와 같은 법 시행령 제14조에 따라 개인정보 보호와 관련하여 자율규제를 수행하는 단체(이하 "자율규제 단체"라 한다)의 지정 등에 관한 사항을 정함으로써 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 이를 지원하고자 함을 목적으로 한다.

제2조(적용범위) 다음 각 호의 자는 자율규제단체의 지정·지정취소, 자율규제 협의회 구성 등에 관하여 다른 법령에 특별히 정한 경우를 제외하고는 이 규정에서 정하는 바에 따른다.

1. 제7조에 따라 자율규제단체로 지정된 협회·단체, 자율규제단체에 소속된 개인정보처리자(이하 "소속 개인정보처리자"라 한다)
2. 제16조에 따라 지정된 전문기관

제3조(자율규제단체 등의 책무) 자율규제단체와 소속 개인정보처리자는 자율적인 개인정보보호 활동을 함에 있어서 다음 각 호 사항을 준수하여야 한다.

1. 상호 합의에 기초
2. 자발적인 참여
3. 공정하고 투명한 활동
4. 개인정보보호 자율규제 활동을 위한 노력

제2장 자율규제 협의회

제4조(자율규제 협의회) 행정자치부장관은 자율규제단체 지정 등에 관한 다음 각 호의 업무를 위하여 개인정보보호 자율규제 협의회(이하 “협의회”라 한다)를 둘 수 있다.

1. 자율규제단체의 지정 및 지정 취소에 대한 심사
2. 제11조의 자율규제 규약에 대한 검토
3. 제15조의 개인정보보호 자율규제 계획 및 활동에 대한 검토
4. 그 밖에 자율규제단체의 개인정보 보호 활동에 관하여 필요한 사항

제5조(협의회 구성 등) ① 협의회는 행정자치부, 개인정보보호위원회, 보건복지부, 국토교통부, 전문기관 및 전문가로 구성하며 위원은 다음 각 호에 해당하는 자로 한다.

1. 행정자치부, 개인정보보호위원회, 보건복지부, 국토교통부 소속 개인정보보호 업무를 담당하는 국장급 공무원
2. 제16조에 따라 전문기관으로 지정된 기관의 개인정보 보호 업무를 담당하는 임직원
3. 개인정보 보호와 자율규제에 관하여 학식과 경험이 풍부한 민간 전문가 5인 이내
4. 위원장이 개인정보보호 자율규제단체 지정 등의 업무를 효율적으로 운영하기 위해 지정한 협회·단체 소관 행정기관의 국장급 공무원

② 위원장은 협의회의 업무를 총괄하며 제1항제3호 민간 전문가 1인으로 정한다.

③ 간사는 제16조제2항에 따라 지정된 한국인터넷진흥원 개인정보보호 자율규제 업무를 담당하는 자로 한다.

④ 제1항제3호 위원 임기는 2년으로 하되, 연임할 수 있다.

⑤ 협의회의 회의는 위원장이 필요하다고 인정하거나 재적 위원 3분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

제6조(행정기관 등에 대한 협조요청) ① 협의회는 직무수행을 위하여 필요한 경우 행정기관이나 전문기관 또는 전문가의 의견 청취, 자율규제단체에 자료 및 의견 제출 등의 협조를 요청할 수 있다.
② 행정기관이나 자율규제단체는 제1항에 따른 요청을 받은 경우 이에 적극 응하여야 한다.

제3장 자율규제단체의 지정 등

제7조(자율규제단체의 지정) ① 자율규제단체로 지정받고자 하는 협회·단체는 [별지 제1호]의 자율규제단체 지정신청서를 협의회에 제출하여야 한다.
② 협의회는 제1항의 신청서를 제출한 협회·단체가 자율적 개인정보 보호활동 역량이 있는지 여부에 대하여 심사한다.
③ 행정자치부장관은 제2항의 심사 결과에 따라 자율규제단체를 지정 확정한다.
④ 행정자치부장관은 제3항에 따라 [별지 제2호]의 자율규제단체 지정서를 발급하고 홈페이지 게시 등의 방법으로 지정 사실을 공개하여야 한다.

제8조(자율규제단체의 지정 취소) ① 협의회는 자율규제단체가 다음 각 호의 어느 하나에 해당하는 경우 자율규제단체 지정 취소를 심사할 수 있다.

1. 허위 또는 부정방법으로 제7조의 지정을 받은 경우
2. 자율규제단체의 수행실적 관련 보고 및 제출을 하지 않은 경우
3. 자율규제단체 운영을 통해 알게된 정보를 부당하게 이용한 경우
4. 권한 오남용, 직무상 의무 위반 등 자격유지가 부적합하다고 인정되는 경우

② 자율규제단체는 자율규제단체 지정의 취소를 원하는 경우 지정의 취소를 행정자치부장관에 신청할 수 있다.
③ 행정자치부장관은 제1항의 심사 결과나 제2항의 지정의 취소 신청에 따라 자율규제단체를 지정 취소할 수 있다.

제9조(자율규제단체의 추가 지정) ① 협의회 또는 행정기관 등은 자율규제 활동의 수요 및 필요성 등을 고려하여 자율규제단체를 추가로 지정할 것을 행정자치부장관에게 요청할 수 있다.
② 행정자치부장관은 제1항에 따라 자율규제단체를 추가 지정할 수 있으며, 이 경우 대상 협회·단체가 쉽게 확인할 수 있도록 홈페이지 및 공문 등을 통해 일정 및 절차 등을 안내하여야 한다.
③ 자율규제단체의 추가 지정 기준 및 절차 등은 제7조에 따른다.

제4장 자율규제단체의 업무

제10조(자율규제단체의 업무) 자율규제단체는 소속 개인정보처리자를 대상으로 다음 각 호의 업무를 수행하도록 노력하여야 한다. 이 경우 제1호 및 제2호는 반드시 수행하여야 한다.

1. 개인정보 보호 교육 및 홍보 활동
2. 개인정보 보호 자율규제 규약 제정
3. 개인정보 자율점검 및 컨설팅
4. 개인정보 보호 관리 시스템의 설치 및 운영
5. 그 밖의 개인정보 보호에 관한 업무

제11조(자율규제 규약) ① 자율규제단체는 소속 개인정보처리자의 개인정보 처리 특성을 고려하여 개인정보 보호에 필요한 규약(이하 “자율규제 규약”라 한다)을 작성하고 공표하여야 한다.

② 자율규제단체는 소속 개인정보처리자가 자율규제 규약을 적용하고 이를 준수하도록 지도, 권고 등 필요한 조치를 할 수 있다.
③ 소속 개인정보처리자는 자율규제 규약을 준수하도록 노력하여야 한다.

제12조(자율점검) ① 자율규제단체는 자율규제 규약에 따라 소속 개인정보처리자의 개인정보 처리 실태를 점검하고 미흡한 점을 개선하도록 지도할 수 있다.
② 자율규제단체는 제1항의 실태 점검을 하기 최소 1개월 전에 소속 개인정보처리자가 스스로 개인정보 처리 실태를 점검할 수 있도록 표준 자율점검표를 마련하여 배포하여야 한다.

제13조(소속 개인정보처리자) 소속 개인정보처리자는 개인정보보호 자율규제 활동에 대하여 자율적으로 참여 여부를 선택할 수 있다.

제14조(수행 결과 보고의무 등) ① 자율규제단체는 개인정보보호 자율규제 수행 결과를 년 1회 협의회에 보고하여야 한다.
② 자율규제단체는 행정자치부 및 협의회의 자율규제 수행 관련 의견 및 자료 요청에 적극적으로 응하여야 한다.

제5장 자율규제단체에 대한 지원

제15조(수행계획에 따른 결과의 평가 등) ① 협의회는 자율규제단체의 개인정보보호 자율규제 수행계획에 따른 결과를 평가 할 수 있다.
② 행정자치부장관은 제1항에 따른 평가 결과가 우수한 자율규제단체 및 개인정보처리자에 대하여 포상 할 수 있다.
③ 소속 개인정보처리자가 자율규제 규약에 따라 자율점검을 수행하고 개선사항을 성실하게 추진하는 경우 행정자치부장관은 법제63조 개인정보 관련 실태 점검시 행정처분에 대한 유예를 시행 할 수 있다.

제16조(전문기관의 지정 등) ① 행정자치부장관은 자율규제단체 지정, 자율규제단체의 개인정보보호 활동 등 관련 업무의 지원을 위하여 전문기관을 지정하고 해당 업무를 위탁할 수 있다.

② 제1항에 따른 전문기관은 한국인터넷진흥원으로 한다.

③ 행정자치부장관은 협회·단체에 특별한 전문성이 필요로 하는 경우 제1항의 전문기관을 추가하여 지정 할 수 있다.

제17조(업무의 지원) 행정자치부장관은 자율규제단체의 업무 수행에 필요한 다음 각 호의 사항을 지원할 수 있다.

1. 개인정보 보호 전문 인력 파견, 자율점검 지원
2. 개인정보 보호 전문교육, 인식제고 교육 실시
3. 웹 취약점 점검, 보안도구의 제공 등의 기술지원

※ 다만, 보안도구 제공 등 일부 기술지원은 '중소기업기본법 제2조'에 따른 중소기업에만 해당

4. 개인정보 보호 관련 정보 제공 등

부 칙

제1조(시행일) 이 규정은 공표한 날부터 시행한다.

제2조(자율규제단체 지정에 관한 경과조치) 이 규정 시행일 이전에 자율규제단체로 지정된 협·단체는 이 고시에 의하여 자율규제단체로 지정된 것으로 본다.

제3조(재검토기한) 행정자치부장관은「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 규정을 공표한 후 법령이나 현실여건의 변화 등을 검토하여 이 규정의 폐지, 개정 등의 조치를 하여야 하는 기한은 2018년 12월 31일까지로 한다.

■ 개인정보보호 자율규제단체 지정 등에 관한 규정 [별지 제1호서식]

개인정보보호 자율규제단체 지정신청서

접수번호	접수일	처리기간 2개월

신청인	협·단체명 및 대표자 성명	협·단체 설립일	
	주소	전화번호	
협·단체 사항	협·단체 소관부처	소관부처 담당자	
	소관부처 담당자 전화번호	전체 회원사(개인정보처리자) 수	회원사(개인정보처리자) 업종
관리능력 · 단체역량	담당 조직 · 인력	개인정보 가용 예산 규모	
	담당자 성명	담당자 전화번호	

개인정보 보호 자율규제단체 지정을 위와 같이 신청합니다.

년 월 일

신청인

(회사 직인 또는 인감)

행정자치부장관 귀하

첨부서류	개인정보보호 자율규제 수행 계획(추진의지, 실행조직및재원, 활동실적 및 계획 등)

처리절차

신청 안내	→	신청서 작성	→	접 수	→	요건 검토	→	지정·공표
한국인터넷진흥원		신청인		한국인터넷진흥원		자율규제협의회		행정자치부

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보보호 자율규제단체 지정 등에 관한 규정 [별지 제2호서식]

제 호

개인정보 보호 자율규제단체 지정서

1. 협회(단체)명 :

2. 사업자등록번호 :

3. 주 소 :

4. 대 표 자 :

5. 지정조건 :

「개인정보보호 자율규제단체 지정 등에 관한 규정」제7조제3항에 따라 귀 협회(단체)를 자율규제단체로 지정합니다.

년 월 일

행 정 자 치 부 장 관 직인

210㎜×297㎜[보존용지 120g/㎡]

해설서, 가이드라인

2015.2.

개인정보의 안전성 확보조치 기준 해설서

행정자치부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

개인정보의 안전성 확보조치 기준 해설서

본 기준 해설서는 “개인정보 보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적 · 관리적 보호조치 등의 세부 기준 제시를 목적으로 합니다.

Contents

개인정보의
안전성 확보조치
기준 해설서

01 개인정보의 안전성 확보조치 기준 6

02 개인정보의 안전성 확보조치 조문별 해설 14

1. 목적 14
2. 정의 16
3. 내부관리계획의 수립 · 시행 27
4. 접근 권한의 관리 37
5. 접근통제 41
6. 개인정보의 암호화 49
7. 접속기록의 보관 및 점검 56
8. 악성프로그램 등 방지 59
9. 물리적 접근 방지 61
10. 개인정보의 파기 64

03 [붙임] FAQ 70

개인정보의 안전성 확보조치 기준 해설서

개인정보의 안전성 확보조치 기준

제1조(목적)
제2조(정의)
제3조(내부관리계획의 수립·시행)
제4조(접근 권한의 관리)
제5조(접근통제)
제6조(개인정보의 암호화)
제7조(접속기록의 보관 및 점검)
제8조(악성프로그램 등 방지)
제9조(물리적 접근 방지)
제10조(개인정보의 파기)

01 개인정보의 안전성 확보조치 기준

제정 2011. 9. 30. 행정안전부고시 제2011-43호
개정 2014. 12. 30. 행정자치부고시 제2014-7호

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "소상공인"이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.
5. "중소사업자"란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.

7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.

9. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

10. “내부망”이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립 · 시행하는 내부 기준을 말한다.

12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.

17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

제3조(내부관리계획의 수립 · 시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립 · 시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제9조(물리적 접근 방지) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출 · 입 통제를 위한 보안대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

부칙 <제2011-43호, 2011. 9. 30.>

제1조 이 기준은 고시한 날부터 시행한다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치 · 운영 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙 <제2014-7호, 2014. 12. 30.>

이 기준은 고시한 날부터 시행한다.

개인정보의 안전성
확보조치 기준 해설서

개인정보의 안전성 확보조치 조문별 해설

1. 목적
2. 정의
3. 내부관리계획의 수립·시행
4. 접근 권한의 관리
5. 접근통제
6. 개인정보의 암호화
7. 접속기록의 보관 및 점검
8. 악성프로그램 등 방지
9. 물리적 접근 방지
10. 개인정보의 파기

02 개인정보의 안전성 확보조치 기준

1. 목적

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

취지

- 개인정보 보호법 제24조 제3항 및 제29조와 같은 법 시행령 제21조 및 제30조에 근거한 기준으로서, 법률 및 시행령의 규정을 구체화하여 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손 등이 되지 아니하도록 안전성을 확보하기 위한 세부적 기준 제시를 목적으로 한다.

해설

- 이 기준은 모든 개인정보처리자에게 적용된다. 따라서 업무를 목적으로 개인정보를 처리하는 모든 공공기관, 법인, 단체 및 개인 등은 이 기준을 준수하여 개인정보의 안전성 확보에 필요한 조치를 이행하여야 한다

TIP

- 개인정보 보호법 제2조에서 “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등으로 정의함
  - 개인정보 보호법은 개인정보 보호를 위한 일반법이므로 개인정보를 수집, 이용, 제공 등 처리하는 모든 자에 적용될 수 있도록 “개인정보처리자”의 개념을 폭넓게 정의

    : 공공기관, 영리목적의 민간분야 사업자, 협회 · 동창회 등 비영리 기관 · 단체를 모두 포괄

    ※ 예시 : 중앙행정기관, 중앙선거관리위원회, 국회 등 헌법기관, 정유사, 대형마트, 비디오대여점, 렌트카업체, 부동산중개업자, 자동차매매업자, 학교, 보험회사, 은행, 통신사, 여행사, 항공사, 호텔, 학원, 협회, 동창회, 동호회 등
  - 사적인 영역에서의 개인정보 처리는 배제하기 위하여 판례상 확립된 ‘업무상 목적’으로 ‘개인정보파일을 운용하기 위하여’ 개인정보를 처리하는 자로 한정

    ※ 예시 : 사적인 친분관계를 위하여 개인이 휴대폰에 저장한 연락처 정보, 이메일 주소록 등

2. 정의

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.
5. “중소사업자”란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 제1호 및 제2호에 해당하는 자를 말한다.
7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.
9. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
10. “내부망”이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립 · 시행하는 내부 기준을 말한다.
12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진

자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.
17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

취지

- 법 제2조(정의)에서 정의한 용어 이외에 같은 법 시행령과 「개인정보의 안전성 확보조치 기준」의 신규 용어에 대한 해석상의 혼란을 방지하기 위함이다.

해설

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

- “정보주체”는 처리되는 정보에 의하여 알아볼 수 있는 사람으로서, 개인정보 보호법에 의해 보호대상이 되는 존재를 말한다.

2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

- “개인정보파일”은 개인의 이름이나 고유식별자 등을 사용하여 색인 · 분류되어 있는 등 일정한 기준에 따라 쉽게 개인정보를 검색할 수 있도록 체계적으로 배열 또는 구성된 개인정보의 집합물을 말한다.

3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

- “개인정보처리자”란 법 제2조제5호에 따라 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회 · 동창회 등 비영리기관 · 단체, 개인 등을 말한다.
- “개인정보 처리”란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
- “공공기관”이란 법 제2조제6호 및 시행령 제2조에 따른 기관을 말한다.

[개인정보 보호법 제2조제6호]

제2조(정의) 이법에서 사용하는 용어의 정의는 다음과 같다.

6. “공공기관”이란 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체

나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

4. “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.

■ “소상공인”은 “소기업 및 소상공인 지원을 위한 특별조치법”의 제2조제2호에서 정의하고 있는 사업자로서, ‘광업 · 제조업 · 건설업 및 운수업’의 경우에는 10인 미만의 사업자, 그 외의 업종의 경우에는 5인미만의 사업자를 말한다.

[소기업 및 소상공인 지원을 위한 특별조치법 제2조]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “소기업”이란 「중소기업기본법」 제2조제2항에 따른 소기업을 말한다.
2. “소상공인”이란 소기업 중 상시 근로자가 10명 미만인 사업자로서 업종별 상시 근로자 수 등이 대통령령으로 정하는 기준에 해당하는 자를 말한다.

[전문개정 2011.5.24.]

[소기업 및 소상공인 지원을 위한 특별조치법 시행령 제2조]

제2조(소상공인의 범위 등) ① 「소기업 및 소상공인 지원을 위한 특별조치법」(이하 “법”이라 한다) 제2조제2호에서 “업종별 상시 근로자 수 등이 대통령령으로 정하는 기준에 해당하는 자”란 주된 사업에 종사하는 상시 근로자의 수가 다음 각 호의 어느 하나에 해당하는 사업자를 말한다.

1. 광업 · 제조업 · 건설업 및 운수업의 경우: 10명 미만
2. 제1호 외의 업종의 경우: 5명 미만

② 제1항에 따른 주된 사업의 기준과 상시 근로자의 범위 및 인원 산정방법에 관하여는 「중소기업기본법 시행령」제4조 및 제5조를 준용한다.

③ 중소기업청장은 소기업 또는 소상공인에 해당하는지를 확인하기 위하여 필요하다고 인정하는 경우에는 그 확인 방법 및 절차에 관한 사항을 따로 정하여 고시할 수 있다.

[전문개정 2013.12.24]

5. “중소사업자”란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.

6. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.

- “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조와 시행령 제32조에 따른 지위에 해당하는 자를 말한다.
- 법령에서 특정한 지위를 갖는 자가 개인정보 보호 업무를 총괄하거나 업무처리를 최종 결정하도록 정하고 있는 것은 사내의 중요 의사결정을 수행하는 중역으로서 개인정보 보호 요구사항을 적극적으로 반영할 수 있도록 하기 위함이다.

7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

- “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

  ※ ‘개인정보취급자’는 기업 · 단체 · 공공기관의 임직원, 외부기관에서 또는 외부기관으로 파견된 근로자, 계약직원, 아르바이트 직원 등의 시간제근로자 등이 해당될 수 있다.

8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.

- 정보통신망은 전기통신기본법 제2조제2호에 따라 전기통신을 하기 위한 기계 · 기구 · 선로 등 기타 전기통신에 필요한 설비를 이용하거나 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를

수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 의미한다.

9. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

- "개인정보처리시스템"이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.
- 개인정보처리시스템은 일반적으로 개인정보의 체계적인 처리를 위한 DBMS (Database Management System)을 말한다.

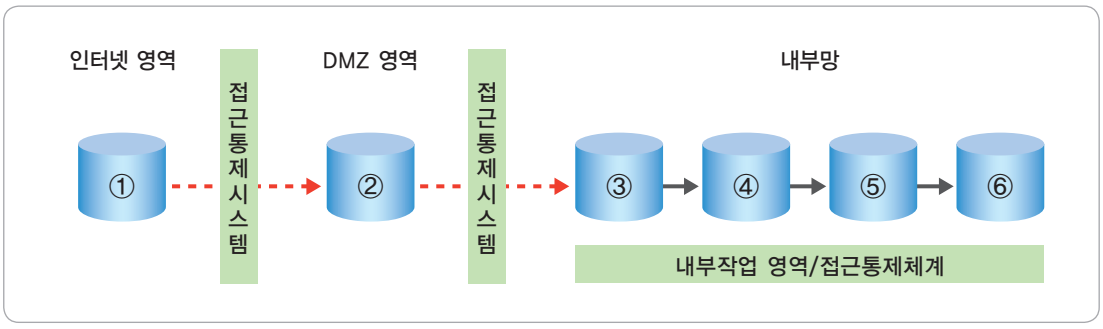
TIP

- 데이터베이스(DB) 응용프로그램이 설치 · 운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외된다.

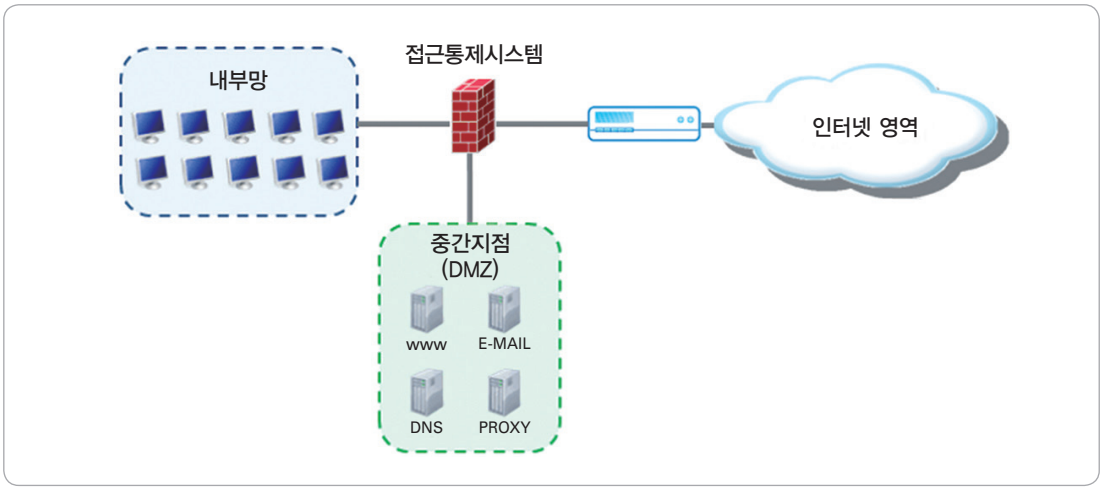
10. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

- "내부망"이란 인터넷 구간과 물리적으로 망이 분리 되어 있거나, 비인가된 불법적인 접근을 차단하는 기능 등을 가진 접근통제시스템에 의하여 인터넷 구간에서의 직접 접근이 불가능하도록 통제 · 차단되어 있는 구간을 말한다.

[내부망 구성도 예시 1]



[내부망 구성도 예시 2]



11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립 · 시행하는 내부 기준을 말한다.

- ‘내부관리계획’은 개인정보처리자가 정보주체의 개인정보를 보호하기 위하여 수립하는 것으로 기본 지침 또는 계획을 의미한다. 내부관리계획에는 개인정보처리자가 취급하는 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 안전성을 확보하기 위한 개인정보 보호 교육 · 감사 등 개인정보 보호 활동에 대한 조직 내부의 개인정보 관리내용 등을 포함하여야 한다.

12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

- ‘비밀번호’는 허가 없이 개인정보처리시스템 또는 업무용 컴퓨터에 인가된 사용자만 접속할 수 있도록 하기 위한 대책의 한 가지로서, 정보주체 또는 개인정보취급자가 컴퓨터 시스템 또는 통신망에 접속할 때 사용자 ID와 함께 입력하여 정당한 사용자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열이다. 회원제로 운영되는 온라인 정보 서비스의 경우, 비밀번호가 없으면 이용할 수 없으며, 서비스 제공자는 입력된 사용자 ID와 비밀번호를 시스템에 등록되어 있는 것과 대조하여 일치해야 접속을 허용하게 된다.

■ ‘타인에게 공개되지 않는 정보’의 의미는 개인정보취급자 중 계정관리자라 할지라도 정보주체 및 개인정보취급자의 비밀번호를 알 수 있는 형태로 관리되어서는 안 된다는 것이다. 비밀번호가 알 수 있는 형태로 관리되는 경우 해당 정보에 접근할 수 있는 내부자, 해커 등의 외부공격자 등에 의한 도용이 가능하기 때문이다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

■ “접속기록”은 개인정보취급자, 개인정보처리자 등이 개인정보처리시스템에 접속하여 운영하였던 이력정보로서, 시스템 식별 · 인증 정보(일시, 컴퓨터 · IP 명, 접속지역, ID 등), 서비스 이용정보(생성, 수정, 삭제, 검색, 출력 등) 등이 개인정보처리시스템에 있는 로그 파일에 자동으로 기록되는 것이다.

■ ‘접속하여 수행한 업무 내역’이라 함은 개인정보취급자가 개인정보처리시스템을 이용하여 수행한 업무를 알 수 있는 정보이다. 개인정보처리자 측면에서는 정보주체의 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등의 업무를 의미한다.

■ ‘식별자, 접속일시, 접속지를 알 수 있는 정보’는 접속한 사실을 확인하는데 필요한 정보를 말한다. 개인정보취급자의 사용자 계정 또는 사용자명 등이 식별자에 해당하며, 접속일시는 접속한 시점 또는 업무를 수행한 시점의 “년-월-일, 시:분:초”가 해당된다. 접속지를 알 수 있는 정보로는 개인정보처리시스템에 접속한 자의 PC 또는 서버의 IP 주소를 의미하며, 접속기록상의 “수행업무”는 개인정보에 대한 수집, 저장, 검색, 출력, 복사, 제공, 공개, 파기 등의 행위 중 어떤 행위를 수행했는지를 알 수 있는 구체적인 정보를 의미한다.

TIP

- 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, ‘수행업무’에는 해당 정보주체를 식별할 수 있는 정보도 포함된다.

■ ‘전자적으로 기록한 것’의 의미는 개인정보취급자가 수기로 작성한 문서가 아니라 시스템 로그와 같이 자동적으로 기록된 정보를 의미한다.

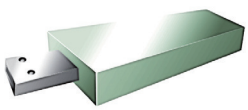
14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

- 지문, 얼굴, 홍채, 정맥, 음성, 필적 등의 바이오정보는 각 개인마다 고유의 특징을 가지기 때문에 개인을 식별하는 정보로 사용되며, 이러한 바이오정보는 신체적 특징과 행동적 특징을 기반으로 생성된 정보로 다음과 같은 것들이 있다.
  - 신체적 특징 : 지문, 얼굴, 홍채, 정맥, 음성, 망막, 손 모양, 손가락 모양, 열상 등
  - 행동적 특징 : 필적, 키보드 타이핑, 입술 움직임, 걸음걸이 등
- 바이오정보는 사람의 신체적 또는 행동적 특징을 입력장치를 통해 최초로 수집되어 가공되지 않은 ‘원본정보’와 그 중 특정 알고리즘을 통해 특징만을 추출하여 생성된 ‘특징정보’로 구분된다.

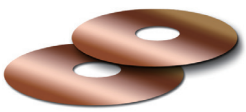
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

- “보조저장매체”는 컴퓨터에 장착된 하드디스크 등의 저장매체 이외에 전자적으로 자료를 저장할 수 있는 매체로서 이동형 하드디스크, SSD(Solid State Drive), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓, 자기 테이프 등 개인정보처리시스템, 업무용 컴퓨터 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

[보조저장매체 예시]



[USB메모리]



[CD]

[이동형 하드디스크]

16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.

■ “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

TIP

• “위험도 분석”을 위한 세부 기준은 행정자치부에서 공고한 “개인정보 위험도 분석 기준 및 해설서”로서, 개인정보보호 종합지원 포털(http://www.privacy.go.kr)의 자료마당에서 다운로드 할 수 있다.

17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

■ “모바일 기기”는 이동통신망, Wi-Fi 등의 무선망을 이용하여 개인정보 처리에 이용되는 휴대용 기기로서, 이러한 기기에는 스마트폰, 태블릿PC, PDA(Personal Digital Assistant) 등이 있다.

[모바일 기기 예시]

[스마트폰]

[태블릿 PC]

[PDA]

■ “개인정보 처리에 이용되는 휴대용기기”의 의미는 개인정보처리자가 업무를 목적으로 개인정보취급자로 하여금 개인정보 처리에 이용하도록 하는 휴대용 기기를 말한다.

– 개인 소유의 휴대용기기라 할지라도 개인정보처리자의 업무 목적의 개인정보 처리에 이용되는 경우 모바일 기기에 포함된다.

TIP

• 개인정보처리자의 ①“업무 목적”으로 ②“개인정보를 처리”에 이용되지 않는 휴대용기기는 “모바일 기기”에서 제외된다.

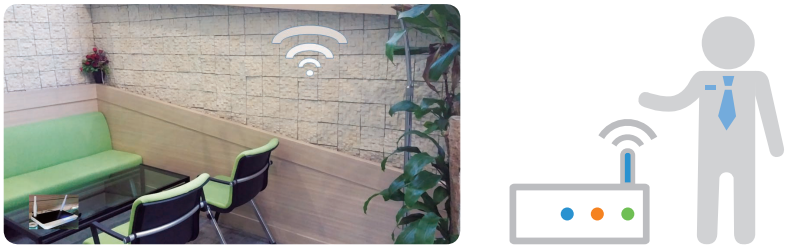
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

■ “공개된 무선망”이란 공개된 장소 등에서 불특정 다수가 무선 접속장치(AP)를 통해 인터넷을 이용할 수 있는 망을 의미한다.

※ 무선접속장치(AP: Access Point) : 와이파이(Wi-Fi), 블루투스 관련 표준을 이용하여 유선 장치(예: 유선 LAN)와 무선 장치(예: 무선 LAN)를 연결시켜주는 컴퓨터 네트워크 장치중의 하나로서, 두 장치간 데이터를 중계할 수 있으며 라우터, 이더넷 허브 등에 연결하여 사용할 수 있다.

– 예를 들어, 커피전문점, 도서관, 병원 등에서 여러 방문객이나 고객이 인터넷을 이용할 수 있도록 무선접속장치(AP)를 설치 · 운영하는 망의 경우 “공개된 무선망”에 해당한다.

[공개된 무선망(커피전문점) 예시]



TIP

• 개인정보처리자가 업무 목적을 위해 개인정보취급자용 무선접속장치(AP)를 설치하여 운영하는 경우 “공개된 무선망”에서 제외된다.

예) 회사가 사무실, 회의실 등에서 직원 업무용 무선접속장치(AP)를 설치 · 운영하는 경우의 무선망

■ “공개된 무선망”이 설치된 장소의 예로는 커피전문점, 도서관, 공항, 철도역, 버스터미널, 대학, 병원, 유통센터, 호텔, 이동통신사, 개인정보처리자 등이 다수 고객이나 방문객용으로 무선접속장치(AP)를 설치한 매장, 로비, 대합실, 회의실, 휴게실, 주차장 등의 장소가 이에 해당한다.

TIP

• CDMA, WCDMA 등의 기술을 사용하는 이동통신망은 “공개된 무선망”에서 제외된다.

3. 내부관리계획의 수립·시행

제3조(내부관리계획의 수립 · 시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립 · 시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

취지

- 정보주체의 개인정보를 보호하기 위한 조치를 적절히 시행하기 위해서는 개인정보처리자 전체에 통용되는 내부규정이 필요하다. 이를 기초로 세부 지침이나 안내서를 마련하여 개인정보취급자 전원이 동일한 행동을 취할 수 있도록 할 필요가 있다.
- 개인정보처리자는 취급하는 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손 되지 아니하도록 안전성을 확보하기 위하여 개인정보 보호 활동에 대한 조직 내부의 개인정보 관리를 위한 내부관리계획을 수립하고, 개인정보 관련 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.
  - 이와 같이 내부관리계획을 수립하도록 하는 이유는 개인정보 보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으며, 이를 위하여 경영층의 방향제시와 지원이 필수적이다.

해설

- 내부관리계획에는 개인정보 보호 조직의 구성 및 운영에 관한 다음과 같은 사항을 포함하여야 한다.
  - 개인정보 보호책임자의 지정에 관한 사항
  - 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
  - 개인정보의 안전성 확보에 필요한 조치에 관한 사항
    - 제4조(접근 권한의 관리), 제5조(접근통제), 제6조(개인정보의 암호화), 제7조(접속기록의 보관 및 점검), 제8조(악성프로그램 등 방지), 제9조(물리적 접근 방지), 제10조(개인정보의 파기) 등
  - 개인정보취급자에 대한 교육에 관한 사항
  - 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
  - 그 밖에 개인정보 보호를 위하여 필요한 사항
- 내부관리계획은 전사적인 계획내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

TIP

- 내부관리계획의 문서 제목은 가급적 “내부관리계획”이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 상황에 따라 다른 용어를 사용 할 수 있다.
- 공공기관의 경우에는 ‘개인정보 보호 추진계획’이라는 이름으로 용어가 사용되기도 한다.

[개인정보 내부관리계획 목차 (예시)]

제1장 총칙

제1조(목적)

제2조(용어정의)

제3조(적용범위)

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

제5조(내부관리계획의 공표)

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 지정)

제7조(개인정보 보호책임자의 의무와 책임)

제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적 · 관리적 안전조치

제9조(접근권한의 관리)

제10조(접근통제)

제11조(개인정보의 암호화)

제12조(접속기록의 보관 및 점검)

제13조(악성프로그램 등 방지)

제14조(물리적 접근 방지)

제15조(개인정보의 파기)

제5장 개인정보 보호 교육

제6장 수탁자에 대한 관리 및 감독에 관한 사항

제7장 개인정보 침해대응 및 피해구제

1. 개인정보 보호책임자의 지정에 관한 사항

■ 개인정보 보호책임자의 자격요건

- 원칙적으로 법 제31조제1항 및 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO: Chief Privacy Officer) 직제를 신설하거나, 정보주체의 개인정보 보호 업무를 위해 조직된 부서의 장 등을 지정할 수 있다.
- 또는, 개인정보처리자의 사업 환경에 따라 정보주체 개인정보를 주로 활용하는 업무를 수행하는 부서(고객 응대, 마케팅, 경영지원 등)나 정보보호 업무를 수행하는 부서에서 본연의 업무와 동시에 개인정보와 관련된 정보주체의 고충처리를 담당하게 되는 경우 해당 부서의 장이 개인정보 보호책임자에 지정될 수도 있다.
- 조직 내에 정보보호(Security) 업무를 총괄하는 정보보호책임자(CSO: Chief Security Officer)가 별도로 있는 경우에는 기술적 조치에 관하여 상호간의 업무를 분명하게 분장하여야 한다. 개인정보처리자는 개인정보 보호책임자와 정보보호 책임자로 동일인을 지정할 수도 있다.
- 개인정보 보호책임자는 정보보호 관련 지식뿐만 아니라 개인정보 취급에 관한 법 · 제도적인 측면 등의 다양한 지식을 습득할 필요가 있다.

[개인정보 보호법 시행령 제32조 제2항]

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.

1. 공공기관의 경우: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
   - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상당하는 공무원
   - 나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
   - 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원
   - 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
   - 마. 시 · 도 및 시 · 도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원
   - 바. 시 · 군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원
   - 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장으로서 공공기관의 장이 지정하는 사람

2. 공공기관 외의 경우: 다음 각 목의 어느 하나에 해당하는 사람

가. 사업주 또는 대표자

나. 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람

■ 개인정보 보호책임자의 지정

– 개인정보처리자는 개인정보 보호책임자의 자격요건에 부합하는 사람을 개인정보 보호책임자로 지정하여야 한다. 개인정보 보호책임자의 지정 시에는 인사발령 등을 통해 공식적으로 책임과 역할을 부여하여야 한다.

TIP

- 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보 보호책임자를 지정하지 않아도 된다.
- 근거 : 개인정보 보호법 제58조(적용의 일부 제외) ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조(개인정보 보호책임자의 지정)를 적용하지 아니한다.

2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

■ 개인정보 보호책임자의 역할

– 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임지는 역할을 수행하는 사람으로, 개인정보 보호를 위해 개인정보와 관련된 내부지침을 준수하도록 기술적 · 관리적 보호조치를 실시하고 관리 · 감독하는 책임을 진다.

– 또한, 정보주체의 불만사항 접수 및 처리에 대한 책임을 지며, 개인정보를 취급하는 직원에 대해 교육훈련을 실시하여야 한다. 개인정보를 취급하는 업무를 외부에 위탁한 경우, 개인정보 보호책임자는 해당 위탁자의 개인정보 관리현황을 지속적으로 확인해야 한다.

[개인정보 보호법 제31조 제2항]

제31조(개인정보 보호책임자의 지정) ② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 · 감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

[개인정보 보호법 시행령 제32조 제1항]

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제2항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다.

1. 법 제30조에 따른 개인정보 처리방침의 수립 · 변경 및 시행
2. 개인정보 보호 관련 자료의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

■ 개인정보취급자의 역할 및 책임

– "개인정보취급자"는 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자로서 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 해야 한다.

– "개인정보취급자"는 기업 · 단체 · 공공기관의 임직원, 외부기관에서 또는 외부기관으로 파견된 근로자, 계약직원, 아르바이트 직원 등의 시간제근로자 등이 해당될 수 있다.

[개인정보취급자의 역할 및 책임 예시]

- 개인정보 보호 활동 참여
- 내부관리계획의 준수 및 이행
- 개인정보의 안전성 확보조치 기준 이행
- 소속 직원 또는 제3자에 의한 위법 · 부당한 개인정보 침해행위에 대한 점검 등

3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항

- 개인정보의 안전성 확보에 필요한 조치에 관한 사항을 빠짐없이 내부관리계획에 포함해야 한다. 세부내용은 해설서 각 항목에 해당하는 부분을 확인한다.

TIP

- 안전성 확보에 필요한 조치 사항 : 제4조(접근 권한의 관리), 제5조(접근통제), 제6조(개인정보의 암호화), 제7조(접속기록의 보관 및 점검), 제8조(악성프로그램 등 방지), 제9조(물리적 접근 방지), 제10조(개인정보의 파기)

4. 개인정보취급자에 대한 교육에 관한 사항

- 개인정보 보호 교육의 목적은 안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보 보호에 대한 인식을 제고시키고 개인정보 보호 대책의 필요성을 이해시키는 것이다.
- 개인정보처리자는 개인정보 보호책임자 및 개인정보취급자를 대상으로 매년 정기적으로 개인정보 보호 교육을 실시하여야 한다. 특히, 개인정보취급자가 정보주체의 개인정보를 훼손 · 침해 · 누설할 경우에는 중벌에 처해지므로, 교육 시 이러한 점을 개인정보취급자에게 인식시키기 위해 노력해야 한다.
- 개인정보 보호 교육의 구체적인 사항에는 교육을 하는 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하고, 내부관리계획 또는 임직원의 결재를 얻은 "○○년 개인정보 보호 교육 계획(안)"과 같은 문서를 통해 관리하도록 한다.
- 교육 방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수도 있다.

TIP

- 행정자치부가 운영하는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 제공하는 온라인 교육 프로그램, 개인정보 보호 교육교재 등을 활용할 수 있다.

■ 교육내용에는 해당 업무를 수행하기 위한 분야별 전문기술 교육뿐만 아니라 개인정보 보호 관련 법률 및 제도, 사내 규정 등 필히 알고 있어야 하는 기본적인 내용을 포함하여 교육을 실시하도록 한다. 교육내용에 포함될 수 있는 예시는 다음과 같은 사항들이 있다.

[개인정보 보호 교육내용 예시]

- 개인정보 보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인정보처리시스템의 안전한 운영 · 사용법(하드웨어, 소프트웨어 등)
- 개인정보의 안전성 확보조치 기준
- 개인정보 보호 위반을 보고해야 할 필요성
- 개인정보 보호업무의 절차, 책임, 작업 설명
- 개인정보 보호 관련자들의 금지 항목들
- 개인정보 보호 준수사항 이행 관련 절차
- 개인정보 유 · 노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 등 업무절차 등

5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

■ 개인정보처리자는 개인정보 처리업무 위탁시 수탁자에게 제공된 개인정보를 안전하게 관리할 책임이 있다. 따라서 개인정보 처리업무를 위탁하는 경우, 개인정보보호법 제26조 및 동법 시행령에 규정된 사항을 준수하고 수탁자가 개인정보를 안전하게 처리할 수 있도록 수탁자 관리 및 감독에 관한 사항을 내부관리계획에 포함해야 한다.

[개인정보보호법 제26조]

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

■ 개인정보 처리 업무 위탁시 문서화(예: 위탁계약서) 하는 경우 수탁자의 무분별한 개인정보 재위탁, 개인정보 관리 소홀, 개인정보 유출 등을 예방하고 의무 위반시 손해배상 책임 등을 명확하게 하기 위해 다음의 사항을 포함하여 작성하여야 한다.

[개인정보 처리 업무 위탁 문서화(예: 위탁계약서)시 포함사항]

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적 · 관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁 제한에 관한 사항
- 접근통제 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항 등

- 내부관리계획에는 개인정보 처리업무 위탁 문서화 내용에 따라 수탁자 교육, 관리 · 감독이 정확하게 실제적으로 이루어지도록 관련 사항을 구체적으로 포함해야 한다.
  - 예를 들어 내부관리계획에 "수탁자 관리 · 감독"항목을 만들고 여기에 위탁계약서의 각 내용별로 관리 · 감독하기 위한 방법, 절차, 시기, 항목 등을 서술하는 방법이 있다.
- 개인정보처리자는 내부관리계획에 정해진 바에 따라 정기적으로 수탁자에 대해 관리 · 감독 및 교육을 실시하고, 그 결과에 대한 기록을 남겨야 하며 문제점이 발견된 경우 그에 따른 개선 조치를 하여야 한다.

[수탁자 개인정보보호 교육내용 예시]

- 수탁업무의 목적 · 범위, 목적외 개인정보 처리 금지 사항
- 수탁자 개인정보처리시스템 및 업무용 PC의 접근 권한의 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 방지 등 개인정보의 안전성 확보조치 기준
- 수탁받은 개인정보 처리업무의 안전성 확보조치 방법
- 수탁받은 개인정보 처리업무의 목적 달성 또는 계약 해지시 개인정보 파기
- 개인정보취급자의 의무
- 수탁업무와 관련하여 개인정보 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

6. 그 밖에 개인정보 보호를 위하여 필요한 사항

- 개인정보처리자의 개인정보 처리(수집 · 이용 · 저장 · 제공 · 파기 등) 환경 및 중요도(민감정보 처리 등)를 고려하여 보안서약서 작성 등 개인정보 보호를 위하여 필요한 사항을 기술할 수 있다.
- 보안서약서 작성
  - 조직에서 임직원들의 기밀정보 유출 위험을 최소화하고, 임직원에게 개인정보 보호에 대한 책임을 명확히 주지시키기 위해 보안서약서에 서명하도록 한다.
  - 보안서약서의 서명은 개인정보 보호를 위한 기본적인 절차 중 하나로 인식되고 이행될 필요가 있다. 이러한 절차는 일반적으로 신규 인력 채용 시 인력관리 부서에 의해 수행될 수 있다.
  - 보안서약서에는 일반적으로 '고객 개인정보 보호, 회사 영업비밀 보호 등의 의무'에 관한 내용과 서명날짜, 서명자 정보 및 서명을 포함하여야 한다.

4. 접근 권한의 관리

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

취지

- 접근권한 관리의 목적은 개인정보처리시스템에 대하여 업무 목적 외 불필요한 접근을 최소화하고, 인사이동 등 권한 변경 사항 발생에 따른 인가되지 않는 접근을 차단하는데 있다.
- 접근권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여되어야 하며 인사이동이나 권한변경 발생 시 지체없이 해당 권한을 변경 또는 말소 하고, 개인정보 유출 예방 및 대응 등을 위해 개인정보취급자 별로 사용자계정을 발급하여 관리하여야 한다.

해설

① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

■ 개인정보의 분실 · 도난 · 유출 · 변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 필요 최소한의 범위로 업무담당자에게 차등 부여하고 접근통제를 위한 조치를 취해야 한다.

TIP

• 예를 들어 개인정보 보호책임자에게는 전체권한(읽기/쓰기/변경)을 부여하고, 개인정보취급자에게는 일부권한(읽기)만 부여하는 등 접근권한에 차등을 두어야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

■ 조직 내의 임직원 전보 또는 퇴직 등 인사이동 등으로 사용자 계정의 변경 · 말소가 필요한 경우에는 공식적인 사용자 계정 관리절차에 따라 통제될 수 있도록 한다.

– 내부 인력의 퇴직 시 해당 인력의 계정을 지체없이 변경하도록 지침에 반영하여 이행하도록 한다.

– 임직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용계정의 말소 항목을 반영하여, 계정의 말소 여부에 대해 확인을 받을 수 있다.

■ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경, 말소에 대한 내역을 기록하고 해당 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

■ 개인정보처리시스템에 접속할 수 있는 사용자계정은 개인정보취급자 별로 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

– 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 사용자계정을 공유하지

않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임 추적성(Accountability)을 확보하여야 한다.

※ 책임 추적성이란 개인정보 취급에 따른 문제 발생시 사용자계정을 기반으로 책임소재를 파악하는 것을 말한다.

TIP

- 한명의 개인정보취급자가 여러 업무를 수행해야 하는 경우, 해당 개인정보취급자에게 각 업무별로 사용자계정을 발급 할 수 있다.

  (예: 개인정보취급자 1명이 서로 권한이 다른 조회, 삭제 등 2개의 업무 수행시, 조회업무용과 삭제업무용으로 구분하여 2개의 사용자계정 발급 가능)

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

■ 개인정보처리자는 개인정보취급자나 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템 등에 적용하여 운영하여야 한다. 다만, 정보주체의 비밀번호는 정보주체의 편의성 등을 고려하여 개인정보처리자가 자율적으로 적절한 수준을 설정하는 것이 필요하다.

– 비밀번호는 산업스파이, 침입자, 비인가자가 추측하기 어려운 문자와 숫자를 포함하도록 하거나, 전에 사용된 비밀번호를 다시 사용하지 않는 등의 다음과 같은 비밀번호 설정 원칙을 참고하여 생성하도록 한다.

- 비밀번호의 최소 길이 : 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 이는 정보주체에 대한 비밀번호 작성규칙과는 달리 반드시 준수하여야 한다

  ※ 컴퓨터 관련 기술의 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있고, 변경주기는 짧아질 수 있다.

- 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 2종류 이상으로 구성한 경우
- 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

  ※ 특수문자 32개 예시

~ · ! @ # $ % ^ & * ( ) _ – + = [ ] [ ] |

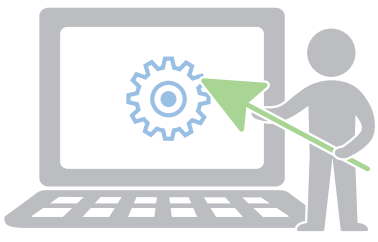
– 추측하기 어려운 비밀번호의 생성 :

  • 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.

  • love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.

– 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.

– 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.



5. 접근통제

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 반드시 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

취지

- 접근통제의 목적은 정보통신망을 통해 개인정보처리시스템에 대한 인가되지 않은 불법적인 접근을 차단하는 것으로, 정보통신망, 인터넷 홈페이지, 업무용 컴퓨터나 모바일 단말 등 개인정보를

처리하는 각 요소에서 적절한 접근통제 정책의 구현을 통해 불법적인 접근이 적절히 차단되어야 한다.

- 이를 위해 정보통신망에서 IP 주소를 통한 비인가자의 접근 제한, 가상사설망(VPN) 등을 이용한 안전한 접속, 인터넷 홈페이지의 취약점 점검, 업무용 컴퓨터 또는 모바일 기기의 보호조치 등의 접근통제 조치가 필요하다.

해설

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

- 개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 아래의 기능을 포함한 장비 설치 · 운영 등의 조치를 하여야 한다.
  - 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한 (침입차단 기능)
  - 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지 (침입탐지 기능)
- 침입차단 및 침입탐지 기능을 갖춘 장비의 설치 방법 예시
  - 침입차단시스템 및 침입탐지시스템을 설치 · 운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.
  - 또한, 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현할 수 있다.
  - 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를 활용함으로써 초기 투자비용 등을 줄일 수 있다.
  - 공개용(무료) 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당

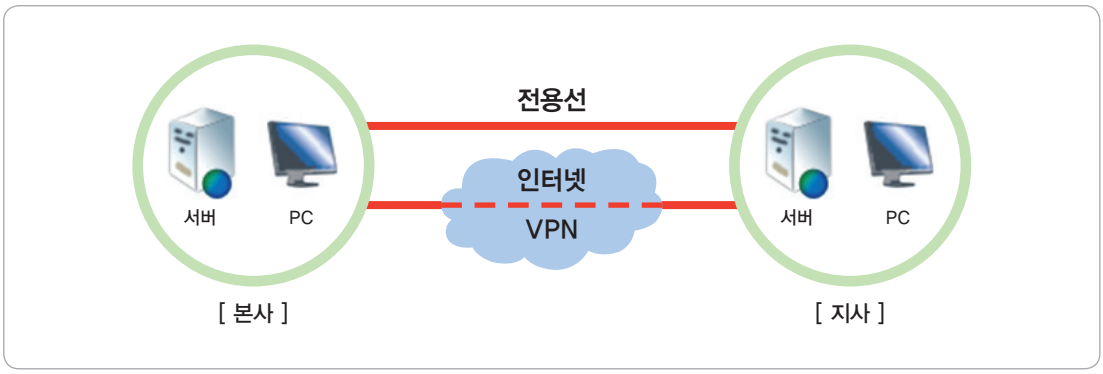
기능을 포함한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하여야 한다.

- 불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비 설치와 더불어 적절한 침입차단 및 침입탐지 정책 설정, 로그 분석 및 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요하다.

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

- 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 한다. 다만 개인정보처리자가 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등의 안전한 접속수단을 적용하여야 한다.
  - 노트북과 같은 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속하는 경우에도 가상사설망, 전용선 등의 안전한 접속수단을 적용하여야 한다.
  - 가상사설망(VPN : Virtual Private Network)은 개인정보 취급자가 사업장 내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안 시스템을 의미한다.
    - ※ IPsec(IP Security Protocol)은 인터넷 프로토콜(IP) 통신 보안을 위해 패킷에 암호화 기술이 적용된 프로토콜 집합
    - ※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜
    - ※ IPsec, SSL 등의 기술이 사용된 가상사설망을 안전하게 사용하기 위해서는, 잘 알려진 취약점(예: Open SSL의 Heart Bleed 취약점)들을 조치하고 사용 할 필요가 있다.

[가상사설망 및 전용선 구성 예시]



③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 이용하는 경우에도 정보주체의 추가적인 정보를 반드시 확인하여야 한다.

- 인터넷 홈페이지에서 성명, 주민등록번호만으로 정보주체의 본인 여부를 확인한 후 서비스를 제공할 경우 해커 등 타인이 유출된 개인정보를 도용하여 서비스를 이용할 수 있다. 이를 방지하기 위해 정보주체의 추가정보를 반드시 확인하여야 한다.
- 정보주체의 추가적인 정보를 확인하는 방법에는 i-PIN, 공인인증서, 휴대전화, 주민등록증 발급일자, 전자우편(e-mail) 주소 등의 수단 중 하나의 수단을 이용한 정보주체의 본인확인, 인증 등이 이에 해당한다.

[추가적인 정보 확인 예시]

[실명확인] [아이핀] [휴대폰] [공인인증서]

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 다음과 같은 항목 등을 고려하여 조치 할 수 있다.
  - 잘 알려진 웹 취약점 항목들을 포함함 웹 취약점 점검 및 조치
    - ※ 웹 취약점 점검 항목 예시 : SQL_Injection 취약점, CrossSiteScript 취약점, File Upload 취약점, ZeroBoard 취약점, Directory Listing 취약점, File Download 취약점 등
    - ※ 잘 알려진 웹 취약점 점검 항목은 행정자치부, OWASP(국제웹표준기구), 국가사이버안전센터(NCSC) 등에서 발표하는 항목 참조
  - 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 삭제 또는 차단 조치

– 관리자 페이지 홈페이지에 대해 노출 차단 등의 보호조치

– 웹 취약점 점검과 함께 정기적으로 웹 쉘 등을 점검하고 조치하는 경우 취급중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다.

■ 개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기에서 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 꼭 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 취급중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 하여야 한다.

– 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.

※ P2P, 웹하드 등의 사용을 제한하는 경우에도 단순히 사용금지 조치를 취하는 것이 아니라 시스템 상에서 해당 포트를 차단하는 등 근본적인 조치를 취하는 것이 필요하다.

■ 개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 취급중인 개인정보가 신뢰되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치(AP)의 취약점 등에 의해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 하며, 다음과 같은 방식들을 활용 할 수 있다.

– 개인정보 송 · 수신시 SSL, VPN 등의 보안기술이 적용된 전용 프로그램을 사용하여 송 · 수신 또는 암호화 송 · 수신

※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 개인정보 전송시, 전송 암호화 기능이 탑재된 별도의 앱(App)이나 프로그램을 설치하고 이를 이용하여 전송

– 개인정보가 포함된 파일 송 · 수신시 파일 암호화 저장 후 송 · 수신

※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 개인정보가 포함된 파일 전송시, 암호화 저장한 후 전송

– 개인정보 유출 방지조치가 적용된 공개된 무선망 이용

※ 예시: 모바일 기기, 노트북에서 설치자를 신뢰할 수 있고 관리자 비밀번호 등을 포함한 알려진 보안취약점이 조치된 무선접속장치(AP)에 안전한 비밀번호를 적용한 WPA2(Wi-Fi Protected Access 2) 보안 프로토콜을 사용하는 공개된 무선망 사용

– 기타

※ 공개된 무선망에서 개인정보 송 · 수신시 유출방지 기술이 적용된 방법 사용

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

■ 인터넷 홈페이지를 통해 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호)를 처리하는 경우에, 개인정보처리자는 고유식별정보가 유출 · 변조 · 훼손되지 않도록 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하여야 하며, 문제점이 발견된 경우 그에 따른 개선조치를 하여야 한다.

– 고유식별정보를 처리하는 인터넷 홈페이지의 웹 취약점 점검시 잘 알려진 웹 취약점 항목들이 포함되도록 할 필요가 있다.

※ 웹 취약점 점검 항목 예시 : SQL_Injection 취약점, CrossSiteScript 취약점, File Upload 취약점, ZeroBoard 취약점, Directory Listing 취약점, File Download 취약점 등

※ 잘 알려진 웹 취약점 점검 항목은 행정자치부, OWASP(국제웹표준기구), 국가사이버안전센터(NCSC) 등에서 발표하는 항목 참조

TIP

• 고유식별정보를 처리하지 않는 인터넷 홈페이지는 연 1회 이상 취약점 점검이 필수는 아니나, 개인정보 유출 등에 대비해서 가급적 취약점 점검을 권장한다.

– 웹 취약점 점검과 함께 시큐어 코딩을 적용하고, 정기적으로 관리자 페이지 노출 및 웹 쉘 등을 점검하고 조치하는 경우 인터넷 홈페이지를 통한 고유식별정보의 유출 · 변조 · 훼손의 위험을 더욱 줄일 수 있다.

■ 인터넷 홈페이지의 취약점 점검시에는 기록을 남겨 책임 추적성 확보 및 향후 개선조치 등에 활용할 수 있도록 할 필요가 있다.

■ 인터넷 홈페이지의 취약점 점검은 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있다.

TIP

• 인터넷 홈페이지 취약점 점검 및 조치에 활용할 수 있는 기술문서는 다음을 포함한 다양한 자료가 있다.

소프트웨어 개발보안 가이드(안전행정부, 2013.11.)
시큐어코딩가이드(C, Java)(행정안전부, 2012.9.)
Web 2.0 정보보호 실무가이드(행정안전부, 2010.5.)
홈페이지 취약점 진단 · 제거 가이드(KISA, 2013.12.)

• 인터넷 홈페이지 취약점 점검을 위해 소상공인, 중소사업자, 비영리단체는 한국인터넷진흥원(KISA)에서 제공하는 무료 웹 취약점 점검 서비스 이용할 수 있으며, 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 점검을 신청할 수 있다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

■ 개인정보처리시스템을 이용하지 않고 단순히 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 저장하는 등의 처리를 하는 경우 운영체제나 보안프로그램에서 제공하는 접근통제 기능을 이용할 수 있다.

– PC, 노트북 등의 업무용 컴퓨터의 운영체제(OS)에서 제공하는 접근통제 기능 설정 방법은 다음과 같으며, 별도의 보안프로그램을 사용하여 접근통제 기능을 설정하고 이용 할 수도 있다.

[업무용 컴퓨터(윈도우의 경우) 방화벽 설정 방법]

• 업무용 컴퓨터 : 제어판 ▶ Windows 방화벽 ▶ Windows 방화벽 설정 또는 해제

※ 업무용 컴퓨터 운영체제에서 제공하는 개인용 방화벽 설정시 외부 IP로부터 시도되는 불법적인 접근 등을 차단한다.

– 스마트폰, 태블릿PC 등 모바일 기기에서도 운영체제(OS)나 별도의 보안 프로그램에서 제공하는 접근통제 기능을 이용할 수 있다.

※ 모바일 기기에서는 불필요한 네트워크 소프트웨어 통제, 인입 포트 차단 등의 접근통제 기능을 제공하는 운영체제를 사용할 수 있으며, 이러한 기능을 제공하지 않거나 보다 확장된 접근통제 기능을 사용이 필요한 경우에는 접근통제 기능을 제공하는 별도의 방화벽 등의 어플리케이션(App)을 설치 · 운영이 필요 할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

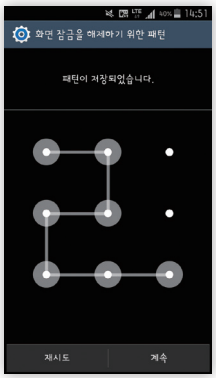
■ 업무용 모바일 기기는 성능이 높아 대량의 개인정보를 저장하거나 전송할 수 있으나, 휴대와 이동이 편리하여 기기 분실 · 도난시 해당 기기에 저장된 또는 해당 기기의 개인정보처리시스템 접속 등을 통한 개인정보 유출의 위험성이 높다.

■ 따라서, 스마트폰, 태블릿PC와 같이 업무에 사용되는 모바일 기기는 분실 · 도난으로 개인정보가 유출되지 않도록 개인정보처리자의 기기 운영 환경 및 처리되는 개인정보의 중요도 등을 고려하여 조치가 필요하며, 다음과 같은 항목들을 조치항목으로 고려 할 수 있다.

– 비밀번호, 패턴, PIN 등을 사용하여 화면 잠금 설정

[화면 잠금 설정 예시]

[비밀번호]



[패턴입력]

– 디바이스 암호화로 애플리케이션, 데이터 등 암호화

– USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금설정

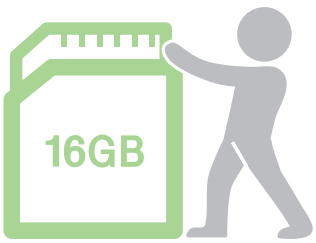
– 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 등의 조치

TIP

• 모바일 기기의 도난 또는 분실 시 원격 잠금, 데이터 삭제 등을 위해 제조사별로 지원하는 '킬 스위치(Kill Switch) 서비스'나 이동통신사의 '잠금 앱 서비스'를 이용할 수 있다.

– 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등의 조치

※ MDM은 무선망을 이용해 원격으로 스마트폰, 태블릿PC 등의 모바일 기기를 제어하는 솔루션으로, 분실된 모바일 기기의 위치를 추적, 원격 잠금 설정, 원격 정보 삭제, 특정 사이트 접속 제한, 카메라 등 기능 제어, 앱 설치 통제 등의 기능 제공



6. 개인정보의 암호화

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

취지

- 비밀번호, 바이오정보, 주민등록번호 등과 같은 주요 개인정보가 암호화되지 않고 개인정보처리시스템에 저장되거나 네트워크를 통해 전송될 경우, 노출 및 위 · 변조 등의 위험이 있으므로 암호화 등의 안전한 보호조치가 제공되어야 한다.

※ "암호화"는 개인정보취급자의 실수 또는 해커의 공격 등으로 인해 개인정보가 비인가자에게 유 · 노출되더라도 그 내용 확인을 어렵게 하는 보안기술이다.

해설

① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

- “고유식별정보”는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호가 여기에 해당한다.
- “비밀번호”는 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
- “바이오정보”는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 최초로 수집되어 가공되지 않은 ‘원본정보’와 가공되거나 생성된 특징정보를 포함한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

- 개인정보처리자는 정보통신망을 통하여 내 · 외부로 송 · 수신 할 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호), 비밀번호, 바이오정보에 대해서는 암호화하여야 한다.

TIP

- 내부망 내에서 송 · 수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화하여야 한다.
- 전용선을 이용하여 개인정보를 송 · 수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등에 대비해서 가급적 암호화 전송을 권장한다.

- 정보통신망을 통한 개인정보 암호화 전송을 위해 SSL 등의 통신 암호 프로토콜이 탑재된 기술을 활용하거나, 개인정보를 암호화 저장한 후 이를 전송하는 방법 등을 사용할 수 있다.

※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜이다.

[SSL 적용 예시]

[일반 웹주소] [SSL 적용 웹주소]

[인증기관(CA)] [SSL설치 웹서버] [사용자]

※ 개인정보 암호화 전송기술 사용시 안전한 전송을 위해 잘 알려진 취약점(예: Open SSL 사용시 HeartBleed 취약점)들을 조치하고 사용 할 필요가 있다.

- "보조저장매체"를 통해 고유식별정보, 비밀번호, 바이오정보를 전달하는 경우에도 암호화 하여야 하며, 이를 위해 다음과 같은 방법 등이 사용 될 수 있다.
  - 암호화 기능을 제공하는 보안USB 등의 보조저장매체에 저장하여 전달
  - 해당 개인정보를 암호화 저장 한 후 보조저장매체에 저장하여 전달

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

- 개인정보처리자는 비밀번호, 바이오정보(지문, 홍채 등)가 노출 또는 위 · 변조되지 않도록 암호화하여 저장하여야 하며, 특히 비밀번호의 경우에는 복호화되지 않도록 일방향 (해쉬 함수) 암호화하여야한다.
- 일방향 암호화는 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.

[일방향(해쉬 함수) 암호화]

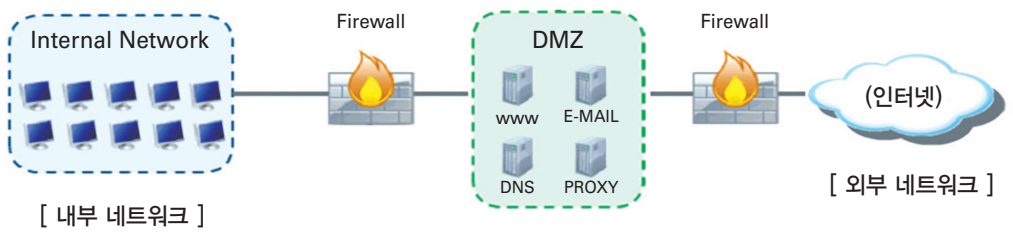
- 일방향(해쉬 함수) 암호화는 입력된 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 길이가 고정된 결과를 만들어 내는 방법을 의미한다.
- 일방향(해쉬 함수) 암호화의 가장 기본적인 성질은 두 해쉬 결과가 다르다면 원래의 데이터도 어딘가 다르다는 것을 의미하며, 원래 입력의 한 비트만 바뀌더라도 해쉬 결과는 크게 달라진다.

■ 바이오정보의 경우, 복호화가 가능한 양방향 암호화 저장이 필요하나, 이는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외된다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

■ 인터넷 구간은 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간, DMZ 구간은 인터넷과 내부망과 인터넷 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말한다. 내부망은 접근통제시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말한다.

[DMZ 구간 예시]



■ 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 이에 따라 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제2항에 따른 비밀번호 및 바이오정보를 저장하는 경우에도 암호화하여 저장해야한다.

■ 주민등록번호를 암호화 저장하는 경우, 속도 등 성능을 고려하여 일부 정보만 암호화 조치를 취할 수 있으며, 이 경우 뒷 자리 6개 번호 이상을 암호화 조치하는 것이 바람직하다.

※ 일부 암호화의 예시: 010101-3******

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

■ 내부망에 고유식별정보를 저장하는 경우, 개인정보 영향평가 및 위험도 분석 결과에 따라 암호화 적용여부 및 적용범위를 정하여 시행할 수 있다.

■ 영 제38조에 따라 영향평가의 대상이 되는 개인정보파일을 운용하는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

– 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행할 수 있다.

■ 다만, 주민등록번호에 대해서는 “개인정보 보호법” 에 따라 2016년 1월 1일부터 내부망에 저장 시에도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따른다.

TIP

• 개인정보 영향평가 수행을 위한 “개인정보 영향평가 수행 안내서” 등의 관련 자료는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.

■ “위험도 분석”은 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

– 세부적으로 위험도 분석은 개인정보 유출에 영향을 미칠 수 있는 다양한 위협에 대한 시스템 취약점과 이로 인해서 예상되는 손실을 분석하여 위험요소를 식별, 평가하고 그러한 위험요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 위험관리의 일부분이다.

– "위험도 분석"은 개인정보를 저장하는 정보시스템에서 개인정보파일 단위로 수행하고 각 개별 개인정보파일의 위험점수에 따라 개별 개인정보파일 단위로 암호화 여부를 결정해야하며, 위험도 분석을 수행한 결과는 최고경영층으로부터 내부결재 등의 승인을 받아야 한다.

TIP

- 위험도 분석을 위한 세부 기준인 "개인정보 위험도 분석 기준 및 해설서"는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

■ 암호화 대상인 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 암호화 하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, "안전한 암호알고리즘"이란 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 권고하는 알고리즘을 의미한다.

TIP

- 안전한 암호알고리즘, 암호화 방식 등은 "개인정보 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.
- 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(http://seed.kisa.or.kr)의 "암호 표준화 및 유관기관"에서도 확인 가능하다.

■ 안전한 암호알고리즘을 사용하더라도 암호화 키가 잘못 관리되어 유 · 노출 되는 경우에는 암호화된 정보들이 유 · 노출될 수 있으므로 이를 안전하게 관리하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

■ 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 업무용 컴퓨터, 모바일 기기에 내려 받아 저장할 때는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화함으로써 불법적인 유·노출 및 접근으로부터 차단하여야 한다.

[오피스에서 파일 암호화 설정방법]

- 한컴 오피스 : 파일 ▶ 다른이름으로 저장하기 ▶ 문서 암호 설정에서 암호 설정 가능
- MS 오피스 : 파일 ▶ 다른이름으로 저장하기 ▶ 도구 ▶ 일반옵션에서 암호 설정 가능

7. 접속기록의 보관 및 점검

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

취지

- 접속기록은 개인정보의 입 · 출력 및 수정사항, 파일별 · 담당자별 데이터접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 불법적인 접근 또는 행동을 확인할 수 있는 중요한 자료이며, 접속기록의 백업은 개인정보 DB의 무결성을 유지하기 위한 중요한 요소이다.
- 따라서, 접속기록을 6개월 이상 안전하게 보관 · 관리하고 반기별 1회 이상 정기적으로 점검하여야 하며, 이를 통해 비정상행위에 대해 적절한 조치를 취할 필요가 있다.

해설

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

- 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등의 접속기록을 6개월 이상 저장하고 정기적으로 확인 · 감독 하여야한다.

[접속기록 항목 예시]

필수 기록 항목	설명
ID	개인정보취급자 식별정보
날짜 및 시간	접속 일시
접속자 IP 주소	접속자 정보
수행 업무	열람, 수정, 삭제, 인쇄, 입력 등

TIP

- 개인정보처리시스템에 접속한 기록이 아닌 경우에는 6개월 보관 · 관리가 필수는 아니다.

  (예: 개인정보처리시스템으로 볼 수 없는 업무용 PC만으로 개인정보 처리시, 이 업무용 PC에 접속한 기록은 6개월 보관 · 관리가 필수는 아님)

– 정보주체에 대한 접속기록까지 보관 · 관리하고 정기적으로 확인 · 감독하는 경우 불법적인 접근 및 비정상 행위에 대한 조치 등을 강화할 수 있다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

■ 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 반기별 1회 이상 정기적으로 점검하여야 한다.

– 이를 통해 비인가된 개인정보 처리, 대량의 개인정보의 조회, 정정, 다운로드, 삭제 등의 비정상 행위를 탐지하여 적절한 대응조치를 할 필요가 있다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

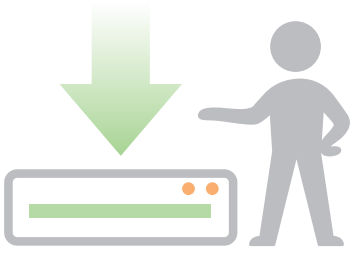
■ 개인정보처리자는 개인정보처리시스템의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.

– 즉, 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하는 등의 조치가 필요하다.

– 접속기록에 대한 위 · 변조를 방지하기 위해서는 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직하다.

– 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위 · 변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관 · 관리할 수 있다.

※ 접속기록을 HDD에 보관하고, 위 · 변조 여부를 확인할 수 있는 정보(MAC 값, 전자서명 값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리할 수 있다.



8. 악성프로그램 등 방지

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

취지

- 악성프로그램이란 제작자가 의도적으로 피해를 주고자 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미하는 것으로 악성 코드라고 불리기도 한다. 컴퓨터 바이러스(Computer Virus), 인터넷 웜(Internet Worm), 트로이목마, 스파이웨어 등의 형태로 나눌 수 있다.
- 악성프로그램은 컴퓨터에서 동작하는 일종의 프로그램으로 자료를 손상 · 유출하거나 프로그램을 파괴하여 정상적인 작업을 방해한다. 이를 방지하기 위해 백신 소프트웨어 등의 보안 프로그램을 이용하여 해당 프로그램을 제거하거나 예방할 필요가 있다.

해설

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

- 개인정보처리자는 악성프로그램 등을 통해 개인정보가 위 · 변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치 · 운영하여야 한다.
- 백신 소프트웨어 등의 보안 프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지해야 한다.
- 백신 소프트웨어 등 보안 프로그램은 자동 업데이트 기능을 사용하거나 일 1회 이상 주기적으로 업데이트를 실시하여 최신의 상태로 유지해야 한다.

– 실시간으로 신종 · 변종 악성 프로그램이 유포됨에 따라 백신 상태를 최신의 업데이트를 적용하여 유지해야 하며, 백신 소프트웨어 등에서 제공하는 자동 업데이트 기능 등을 활용하면 편리하고 신속하게 조치할 수 있다.

– 특히 대량의 개인정보를 처리하거나 민감한 정보 등 중요도가 높은 개인정보를 처리하는 경우에는 키보드, 화면, 메모리해킹 등 신종 악성 프로그램에 대해 대응 할 수 있도록 보안프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지하여야 한다.

[백신 소프트웨어 설정 예시]

[자동, 예약 업데이트]

[실시간, 예약 검사]

2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

■ 운영체제(OS) · 응용 프로그램의 보안 취약점을 악용하는 악성 프로그램 경보가 발령되었거나, 응용 프로그램, 운영체제 제작업체에서 보안 업데이트 공지가 있는 경우에는 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 즉시 업데이트를 실시하여야 한다.

– 운영체제나 응용 프로그램 보안 업데이트시 현재 운영중인 응용 프로그램의 업무 연속성이 이루어 질 수 있도록 보안 업데이트를 적용하는 것이 필요하며, 가능한 자동으로 보안 업데이트가 설정되도록 할 필요가 있다.

※ 한글 Office나 MS Office 등 개인정보처리에 자주 이용되는 응용프로그램은 자동업데이트 설정시, 보안 업데이트 공지에 따른 즉시 업데이트가 용이하다.

9. 물리적 접근 방지

제9조(물리적 접근 방지) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출 · 입 통제를 위한 보안 대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

취지

- 개인정보를 대량으로 보관하고 있는 전산실 · 자료보관실 등 물리적 보관장소를 별도로 가지고 있는 경우, 출입자에 의한 개인정보 대량 유출의 위험이 있으므로 이에 대한 출입통제 절차를 수립하여 운영하고 보조저장매체의 반 · 출입 통제를 위한 보안대책을 마련하여 대응할 필요가 있다.
- 또한 사무실 등에서 개인정보가 포함된 보조저장매체 분실 등으로 인한 개인정보 유출의 위험성이 있으므로 이에 대한 대책 또한 필요하다.

해설

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.

- 개인정보를 대량으로 보관하고 있는 전산실 · 자료보관실을 별도로 두고 있는 경우에는 비인가자의 출입에 의한 개인정보가 포함된 정보자산의 절도, 파괴 등 물리적 위협에 대응하기 위해 출입통제 절차를 수립 · 운영하여야 한다.

- 전산실 · 자료보관실의 출입을 통제하는 방법으로 물리적 접근 방지를 위한 장치를 설치 · 운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하는 방법 등이 있다.
  - 물리적 접근 방지를 위한 장치(예시): 비밀번호 기반 출입통제 장치, 스마트 카드 기반 출입통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
    ※ 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적인 공간으로 전기시설(UPS(Uninterruptible Power Supply), 발전기 등), 공조시설(항온항습기 등), 소방시설(화재감지기, 소화설비 등)등을 갖춘 시설을 의미한다.
    ※ 자료보관실은 가입신청서 등의 문서나 DAT(Digital Audio Tape), LTO(Linear Tape Open), DLT(Digital Linear Tape), CD(Compact Disc), DVD(Digital Versatile Disk), 하드디스크, SSD(Solid State Drive) 등 전자적 기록매체가 다량으로 보관된 물리적 저장장소를 의미한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

- 개인정보처리자는 개인정보가 포함된 서류나 보조기억매체(USB, CD 등) 등은 잠금장치가 부착되어 있는 안전한 장소에 보관하여야 한다.
  - 플로피디스켓, 이동형 하드디스크, USB메모리, SSD, CD, DVD 등의 보조기억매체는 금고 또는 잠금장치가 있는 캐비넷 등에 안전하게 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출 · 입 통제를 위한 보안대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

- 개인정보처리자는 사무실 등 개인정보를 처리하는 업무공간에서 개인정보가 저장된 USB메모리, CD, 이동형 하드디스크 등의 보조저장매체 반 · 출입에 의해 개인정보가 유출되지 않도록 반출 · 입 통제를 위한 보안대책을 마련하여야 한다.
- 보조저장매체 반 · 출입 통제를 위한 보안대책 마련시 다음과 같은 내용이 포함되도록 고려할 필요가 있다.
  - 보조저장매체 보유 현황 파악 및 반 · 출입 관리 계획
  - 개인정보취급자(임직원, 파견근로자, 시간제근로자 등) 및 용역업체의 직원 등에 의한 비인가된 보조저장매체 반 · 출입에 대한 대응

– 개인정보처리시스템, 업무용 PC, 모바일 기기 등에서 보조저장매체의 안전한 사용 방법 및 비인가된 사용에 대한 대응 등

■ 보조저장매체 반 · 출입 통제를 위한 보안대책은 전사적으로 수립되어 운영되도록 할 필요가 있다.

TIP

• 보조저장매체 반 · 출입 통제를 위한 보안대책은 별도의 대책으로 마련 할 수도 있고, 내부관리계획, 지침, 내규 등 다른 관리계획의 일부에 포함될 수도 있다.

■ 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 보조저장매체 반 · 출입 통제를 위한 보안대책 마련이 필수는 아니나, 관련 대책 마련을 권장한다.

※ 예를 들어 소상공인이 사무실에 업무용 PC만 사용하여 개인정보를 처리하는 경우

10. 개인정보의 파기

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형 태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

취지

- 개인정보처리자는 개인정보 수집목적 달성, 보존기간이 경과 등 개인정보가 불필요하게 되었을 때 개인정보의 유출 및 오남용 방지를 위해 개인정보를 복원이 불가능한 방법으로 파기가 필요하다.
  ※ '복원이 불가능한 방법'이란 사회 통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 의미한다.
- 또한, 개인정보 파기 방법 중 개인정보의 일부만 파기시 완전파괴 방법 등을 사용하기 어려운 특정 환경에서도 복구 및 재생되지 않도록 조치하는 방법이 필요하다.

해설

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

■ 개인정보처리자는 개인정보를 파기하는 경우 복구 또는 재생되지 아니하도록 개인정보가 저장된 매체 형태에 따라 다음 중 어느 하나의 조치를 하여야 한다.

– 완전파괴(소각 · 파쇄 등)

※ 예시: 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기하거나 용해, 또는 소각장, 소각로에서 태워서 파기 등

– 전용 소자장비를 이용하여 삭제

※ 예시: 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 등

– 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 예시: 개인정보가 저장된 하드디스크에 대해 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값, 0, 1 등으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등의 방법 사용

TIP

- 개인정보 파기시 파기를 전문으로 수행하는 업체를 활용 할 수 있다.
- 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 파기에 관한 사항을 기록 · 관리하여야 한다.

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

■ "개인정보의 일부만 파기하는 경우"는 저장중인 개인정보 중 보유기간이 경과한 일부 개인정보를 파기하는 경우를 말하며, 다음과 같은 경우 등이 있다.

– 운영 중인 개인정보가 포함된 여러 파일 중, 특정 파일을 파기하는 경우

– 개인정보가 저장된 백업용 디스크나 테이프에서 보유기간이 만료된 특정 파일이나 특정 정보주체의 개인정보만 파기하는 경우

– 운영 중인 데이터베이스에서 탈퇴한 특정 회원의 개인정보를 파기하는 경우

– 회원가입신청서 종이문서에 기록된 정보 중, 특정 필드의 정보를 파기하는 경우 등

■ 개인정보처리자가 개인정보의 일부만 파기하는 경우 복구 또는 재생되지 아니하도록 개인정보가 저장된 매체 형태에 따라 다음 중 어느 하나의 조치를 하여야 한다.

– 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

※ 개인정보를 삭제하는 방법 예시: 운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하여 삭제, 백업시 파기 대상 정보주체의 개인정보를 제외한 백업 등 (운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하는 경우에도 가능한 복구 불가능한 방법을 사용해야 복구 및 재생의 위험을 줄일 수 있다)

※ 복구 및 재생되지 않도록 관리 및 감독하는 방법 예시: 복구 관련 기록 · 활동에 대해 모니터링하거나 주기적 점검을 통해 비인가된 복구에 대해 조치

– 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

※ 예시: 회원가입 신청서에 기재된 주민등록번호 삭제시, 해당 신청서에서 주민등록번호가 제거되도록 절삭, 천공 또는 펜 등으로 마스킹

부칙 <제2011-43호, 2011. 9. 30.>

제1조 이 기준은 고시한 날부터 시행한다.

취지

- 이 고시의 시행일에 대한 정의를 하고 있다. 시행되는 일시는 고시한 날부터이다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치 · 운영 기준이 정하는 바에 따른다.

취지

- 영상정보처리기기에 대한 안전성 확보조치 기준은 「표준 개인정보 보호지침」의 영상정보처리기기 설치 · 운영 기준에서 언급된 안전성 확보조치 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙<제2014-7호, 2014. 12. 30.>

이 기준은 고시한 날부터 시행한다.

개인정보의 안전성 확보조치 기준 해설서

[붙임] FAQ

03 [붙임] FAQ

문1. 개인정보처리시스템의 범위는 어디까지를 말하는지?

개인정보처리시스템은 DBMS(database management system)로서, 다수의 사용자들이 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용프로그램의 집합을 말합니다.

여기에는 DB자체 뿐 아니라, DB에 연결되어 DB를 관리하거나 DB의 개인정보를 처리할 수 있는 응용 프로그램(예: 웹 서버)까지 포함될 수 있습니다.

문2. 개인용 스마트폰에서 회사 e-mail 서버로부터 자료를 주고받아 개인정보 처리 업무를 수행하는 경우에, 모바일 기기에 포함되는지?

모바일 기기에 포함됩니다.

개인용 스마트폰이나 태블릿PC에 회사의 업무용 앱(App)을 설치하여 업무목적의 개인정보를 처리하는 경우나, 개인용 스마트폰이나 태블릿PC에 설치된 메일 읽기 프로그램을 사용하여 회사 메일서버에 접속하여 업무목적의 개인정보를 처리하는 경우에는 모바일 기기에 해당됩니다.

다만, 개인용 스마트폰이 회사 e-mail 서버로부터 자료를 주고 받더라도 개인정보가 포함되지 않거나, 회사 업무목적 아닌 경우는 모바일 기기에서 제외됩니다.

문3. 전용선의 범위는 어디까지 인지?

두 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점간을 직통으로 연결하는 회선 등을 말합니다.

문4. 개인정보처리자로부터 업무를 위탁받아 처리하는 수탁자도 이 기준을 준수하여야 합니까?

그렇습니다.

"수탁자"는 개인정보처리자로부터 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위 등의 업무를 위탁받아 처리하는 자를 말합니다(법 제26조). 그런데 수탁자에 관하여는 개인정보의 안전성 확보조치에 관한 개인정보 보호법 제24조제3항, 제29조가 준용되어 적용됩니다 (법 제26조제7항). 따라서 수탁자는 이 기준에 따라 개인정보의 안전성 확보에 필요한 조치를 이행하여야 합니다.

문5. 「소기업 및 소상공인 지원을 위한 특별조치법」에 따른 소상공인입니다. 내부관리계획을 수립하지 않아도 되는지?

소상공인은 "개인정보의 안전성 확보조치 기준" 제3조제2항에 의거 내부관리계획을 수립하지 않아도 됩니다.

문6. 개인정보 보호에 관한 사항을 회사규칙으로 마련한 경우에도 「개인정보 보호법」에 따른 내부관리계획을 별도로 마련해야 하는지?

회사규칙에 내부관리계획에 포함되어야 하는 내용(개인정보 보호책임자의 지정에 관한 사항, 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항, 개인정보의 안전성 확보에 필요한 조치에 관한 사항, 개인정보취급자 교육에 관한 사항, 수탁자에 대한 관리 및 감독에 관한 사항, 그 밖에 개인정보 보호를 위하여 필요한 사항)이 모두 포함되어 있다면 별도의 내부관리계획을 마련하지 않아도 됩니다.

문7. 비디오 대여점을 운영하는 소상공인입니다. 현재 고객관리를 위해 업무용 컴퓨터를 운영하고 있습니다. "개인정보의 안전성 확보조치 기준"에 따라 어떠한 조치를 수행해야 하는지?

업무용 컴퓨터로 고객정보를 관리하는 경우 제4조(접근 권한의 관리)제5항에 따라 업무용 컴퓨터에 비밀번호를 설정하고 업무용 컴퓨터에서 제공되는 침입차단 기능을 설정하고 악성프로그램을 차단하도록 백신 소프트웨어를 설치하여야 합니다. 또한, 업무용 컴퓨터에 주민등록번호 등 고유식별정보가 저장된 경우에는 암호화 등의 보안조치를 수행하여야 합니다.

문8. 백화점입니다. 고객정보 데이터베이스를 운영하고 있습니다. 개인정보 암호화 대상이 무엇이며 어떻게 해야 하는지?

"개인정보 보호법" 상에서 요구되는 암호화 대상은 고유식별정보(주민등록번호, 외국인등록번호, 운전면허번호, 여권번호), 비밀번호, 바이오정보입니다. 개인정보처리자는 고유식별정보 등을 정보통신망 또는 보조저장매체 등을 통해 전달하는 경우 암호화하여 전송해야 합니다. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에도 반드시 암호화하여야 합니다. 또한, 내부망에 고유식별정보를 저장하는 경우 위험도 분석 또는 영향평가 후에 암호화 적용범위 및 적용범위를 정하여 시행할 수 있습니다.

[암호화 적용 기준 요약표]

<table>
<tr><th colspan="3">구 분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송 · 수신 시</td><td colspan="2">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송 · 수신
※ 내부망에서 전송시 해설 내용 참조</td></tr>
<tr><td rowspan="4">개인정보처리시스템에 저장 시</td><td colspan="2">비밀번호</td><td>일방향 암호화 저장</td></tr>
<tr><td colspan="2">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">고유식별정보</td><td>인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)</td><td>암호화 저장</td></tr>
<tr><td>내부망에 저장</td><td>암호화 저장 또는 다음 항목에 따라 암호화 적용여부 · 적용범위를 정하여 저장
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="2">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 저장(비밀번호는 일방향 암호화 저장)</td></tr>
</table>

다만, 주민등록번호의 경우에는 2016년 1월 1일부터는 내부망에 저장하는 경우라도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따릅니다.

문9. 내부망에 저장하는 주민등록번호는 영향평가나 위험도 분석을 통해 암호화하지 않고 보유할 수 있는지?

2016년 1월 1일 이전까지는 가능하나, 2016년 1월 1일부터 내부망에 저장하는 경우라도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따릅니다.

문10. 암호화해야 하는 바이오정보의 대상은 어디까지 인지?

암호화 하여야 하는 바이오정보는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외됩니다.

바이오정보인 경우에 원본 데이터와 가공되거나 생성된 특징정보 모두 암호화 대상입니다.

문11. 특정기관에서 암호화 관련 준수해야 하는 지침과 본 고시에서 규정한 암호화 요구사항 중 어느 것을 적용해야 하는지?

“개인정보 보호법” 측면에서는 본 고시에서 규정한 암호화 요구사항을 준수하면 “개인정보 보호법”상 암호화 의무는 준수한 것입니다. 본 고시 준수로 인하여 다른 지침을 준수하기 어렵게 된다면 “개인정보 보호법” 은 준수하였으나 해당 지침은 위배한 것이 될 수 있습니다. 따라서, 최선의 방법은 본 고시에서 규정한 암호화 요구사항과 다른 암호화 관련 지침의 요구사항 모두를 준수하는 것이라 할 수 있습니다.

문12. 업무용 PC에서 고유식별정보나 바이오정보를 처리하는 경우 개인정보 암호화는 어떻게 해야 하는지?

PC에 저장된 개인정보의 경우 상용프로그램(한글, 엑셀 등)에서 제공하는 비밀번호 설정기능을

사용하여 암호화를 적용하거나, 안전한 암호화 알고리즘을 이용하는 소프트웨어를 사용하여 암호화해야 합니다.

암호화에 관한 세부 질문사항은 '개인정보 암호화 조치 안내서'를 참고 할 수 있습니다.

문13. 전산실 또는 자료보관실이 없는 중소기업입니다. "개인정보의 안전성 확보조치 기준" 제9조 (물리적 접근 방지)조항을 준수해야 하는지?

기업의 규모에 상관없이 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 운영하고 있지 않으면 출입통제 절차를 수립 · 운영하지 않아도 됩니다.

다만 서류나, 보조저장매체 등을 운영하는 경우에는 잠금장치가 있는 캐비넷 등에 안전하게 보관하여야 하며, 보조저장매체의 반출 · 입 통제를 위한 보안대책을 마련해서 운영해야 합니다.

문14. 접속기록 중, 수행업무에 남겨야 하는 내용은 무엇인지?

접속기록에는 식별자, 접속일시, 접속지를 알 수 있는 정보와 수행업무가 포함됩니다.

수행업무는 정보주체의 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등의 내역을 말합니다.

특히, 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, '수행업무'에는 해당 정보주체에 대한 식별정보도 포함됩니다.

행정자치부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

홈페이지 개인정보
노출방지 안내서

2016.06

행정자치부 한국인터넷진흥원

제 · 개정 이력

본 "홈페이지 개인정보 노출방지 안내서" 는 '08년 2월 제정 이후 5차 개정판입니다.

구분	일자	비고
제정	2008.02	
1차 개정	2009.02	
2차 개정	2011.05	
3차 개정	2012.08	
4차 개정	2014.12	
5차 개정	2016.06	

· 본 안내서는 「개인정보 보호법」 등 관계법령의 규정을 토대로,

  – 개인정보 담당자, 홈페이지 담당자 및 홈페이지 개발자를 대상으로 인터넷에 노출된 개인정보의 오남용을 예방하기 위하여 개인정보 노출 원인별 구체적인 사례 및 조치방법에 대한 올바른 이해를 돕기 위한 목적으로 발간되었습니다.

  – 다만, 다른 사람이 게시하거나 공개한 개인정보를 삭제할 때에는 임의 삭제 조치가 타인의 재산권 침해 등의 우려가 있는지 여부를 반드시 확인 후 조치해야 합니다.

· 본 안내서에서 제공하는 조치방법 및 처리절차 예시 등은 각 기관의 고유한 특성 및 환경에 맞게 적용 하시면 됩니다.

※ 본 안내서는 개인정보보호 종합포털 홈페이지 [www.privacy.go.kr - 자료마당 - 지침자료]와 개인정보보호 포털 [www.i-privacy.kr - 자료실 - 안내서 및 해설서]에 게시될 예정입니다.

CONTENTS

Ⅰ 개요 07

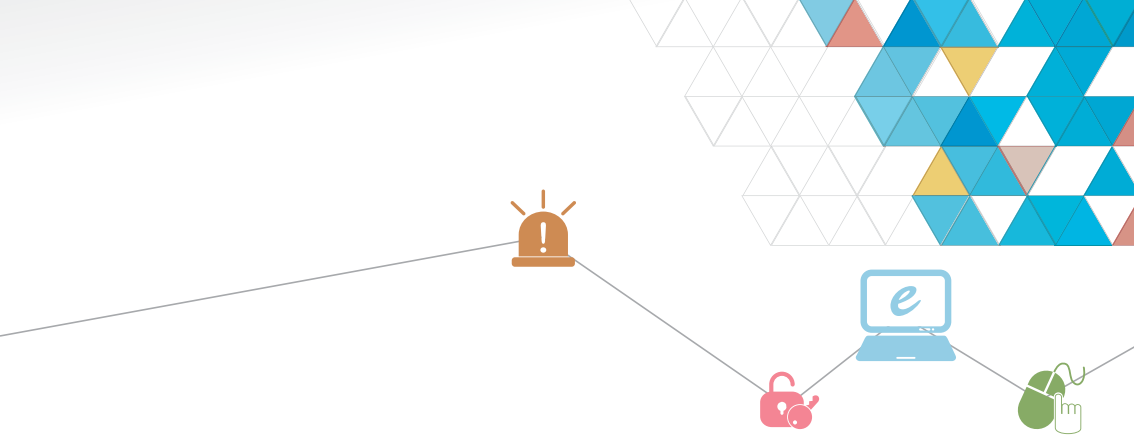
1. 개인정보란? 08
2. 개인정보 노출이란? 10
3. 개인정보 노출 시 어떤 위험이 있나요? 11

Ⅱ 개인정보 노출 원인별 사례분석 13

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 20
2. 첨부파일에 의한 노출 25
3. 게시글에 의한 노출 38

Ⅲ 개인정보 노출 시 조치 방법 41

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법 .. 42
2. 첨부파일이 포함된 게시글 노출 시 조치 방법 53
3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법 55
4. 검색엔진에 저장된 페이지 삭제 방법 공통사항 56



Ⅳ 개인정보 노출 사전에 예방하세요 67

key 1. 첨부파일을 업로드하기 전에 개인정보가 있는지 확인하는 것이 좋습니다.

key 2. 관리자페이지는 안전하게 보호하세요.

key 3. 주기적으로 홈페이지의 개인정보 노출여부를 점검하는 것이 좋습니다.

key 4. 게시글에 비공개 설정 기능이 있는 것이 좋습니다.

key 5. 게시글 작성 시 개인정보 노출주의에 대한 안내를 하는 것이 좋습니다.

용어 정의 71

>>>> 참고 1 홈페이지 개인정보 유출 시 신고절차 76

>>>> 참고 2 OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점 . 86

>>>> 참고 3 구글 웹마스터 도구 사용법 87

>>>> 참고 4 로봇배제표준 98

>>>> 참고 5 고유식별정보 정규표현식 101

Ⅰ 개요

1. 개인정보란?
2. 개인정보 노출이란?
3. 개인정보 노출 시 어떤 위험이 있나요?

Ⅰ 개요

1. 개인정보란?

개인정보란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말합니다. 또한, 해당 정보만으로는 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 경우, 개인정보에 포함됩니다(개인정보 보호법 제2조 제1호). 즉, 하나의 정보 혹은 두 개 이상의 정보들이 모여서 개인을 식별할 수 있다면 개인정보라고 할 수 있습니다.

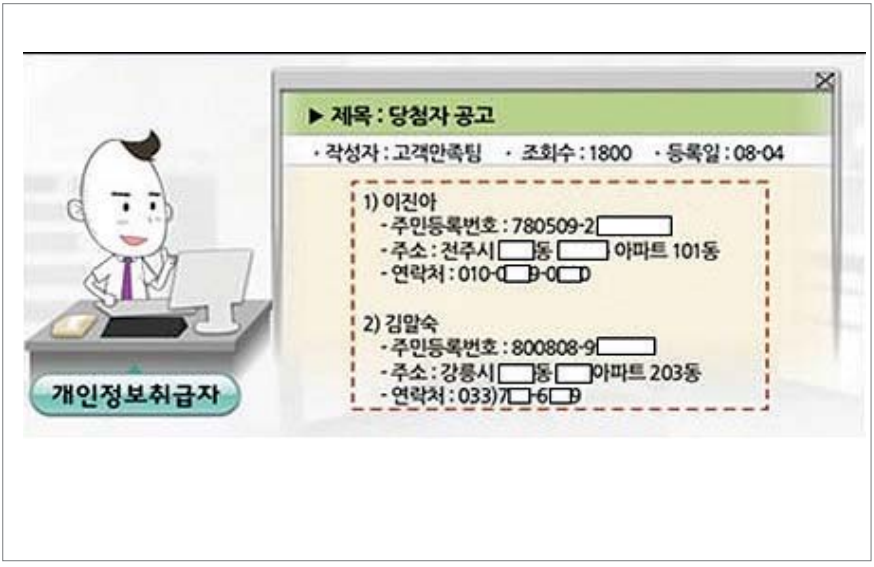
개인정보의 범위는 과거에는 이름, 주민등록번호, 생년월일, 주소 등의 단순한 신분정보를 의미하였으나 오늘날에는 개인의 위치정보, 바이오정보를 비롯한 개인의 기호, 성향, 신념, 사상까지 포함될 정도로 매우 광범위해졌습니다. 이러한 개인정보가 노출되어 악용될 경우 막대한 경제적 · 정신적 피해가 발생할 수 있으므로 홈페이지를 통해 노출되지 않도록 특별히 주의해서 관리해야 합니다.

[표 1] 개인정보의 유형(예)

구분	유형	구분	유형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적	가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 기술 자격증 및 전문 면허증, 학교성적, 동아리활동, 상벌사항, 이수한 훈련 프로그램,	병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등	소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타수익 정보	보험(건강, 생명 등) 가입현황, 병가, 휴가, 회사의 판공비, 투자프로그램, 퇴직프로그램	신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 출석기록, 상벌기록, 성격테스트 결과 직무태도	법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보	조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일(log file), 쿠키(cookies)	위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등	습관 및 취미정보	음주량, 선호하는 스포츠 및 오락, 흡연, 여가활동, 비디오 대여기록, 도박성향

2. 개인정보 노출이란?

개인정보 노출이란 홈페이지를 이용하는 자(이하 홈페이지 이용자)가 해킹 등 특별한 방법을 사용하지 않고, 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷상에서 관련 정보가 방치되어 있는 상태를 말합니다. 노출되는 주요 개인정보는 주민등록번호, 여권번호, 전화번호, 휴대폰번호 등 다양하게 나타날 수 있으며, 이러한 개인정보는 손쉽게 노출이 가능하므로 항상 주의가 필요합니다.



[그림 1] 개인정보 노출 예시

3. 개인정보 노출 시 어떤 위험이 있나요?

개인정보가 노출되면 사생활 침해와 같은 직접적인 피해가 발생할 수 있습니다. 그리고 노출된 개인정보를 신속히 삭제하지 않을 경우, 외부 검색엔진에 의해 노출된 정보가 확산되거나 제3자에게 개인정보가 수집되어 개인정보의 통제권을 상실하게 되므로 2차 피해가 발생할 수 있습니다.

개인의 경우에는 명의도용, 보이스피싱 등에 의한 금전적 손해 및 각종 범죄에 악용될 우려가 있으며, 기업의 경우에는 이미지 실추, 소비자 단체 등의 불매운동, 다수 피해자에 대한 손해배상 등으로 기업경영에 큰 타격을 입을 수 있습니다.

개인정보 노출을 예방하는 최선의 방법은 개인정보 수집을 최소화하는 것입니다. 민감정보와 고유식별정보는 법령에서 규정하고 있거나 정보주체로부터 별도의 동의를 받은 경우에만 수집이 가능합니다. 특히, 주민등록번호는 법령으로 정하거나 급박한 생명 · 신체 · 재산상 이익을 위하여 명백히 필요한 경우만 수집이 가능하고, 정보주체의 동의를 받더라도 수집 · 이용을 할 수 없도록 법령에 명시되어 있습니다.

또한, 보유하고 있던 개인정보가 불필요(보유기간의 경과, 개인정보의 처리 목적 달성 등)하게 되었을 때에는 해당 개인정보를 지체 없이 파기해야 합니다.

개인정보 보호법 상 용어정의

* 민감정보 : 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보(제23조)
  ※ 정보통신망법 적용 사업자는 정보통신망법 제23조 참조/적용/반영
* 고유식별정보 : 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호(시행령 제19조)

※ 2017.03.30.부터 주민등록번호는 법률, 시행령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에 근거가 있어야 처리가능 함 (개인정보 보호법 제24조의2 제①항)

Ⅱ 개인정보 노출 원인별 사례분석

1. 홈페이지 설계 및 관리 미흡으로 인한 노출
2. 첨부파일에 의한 노출
3. 게시글에 의한 노출

Ⅱ 개인정보 노출 원인별 사례분석

홈페이지를 통해 개인정보가 노출되는 주요 원인은 홈페이지 설계 및 관리 미흡, 첨부파일 노출, 게시글 노출이 대부분입니다. 홈페이지 설계 및 관리 미흡에 의한 노출은 시스템 전반에 영향을 미치기 때문에 대량노출로 이어질 가능성이 높으며, 기술적인 조치가 필요한 부분이므로 개발 또는 운영 담당자와 같이 해결해야 합니다.

첨부파일에 의한 노출은 홈페이지 이용자가 첨부파일을 다운로드하여 개인 PC에 저장하는 경우가 많아, 홈페이지 서버에서 해당 첨부파일을 삭제하더라도 이미 외부로 노출된 파일은 삭제할 수 없기 때문에 개인정보가 유출될 위험성이 높습니다.

게시글에 의한 노출은 개인정보 취급자가 공지사항 작성이나 민원 처리 시 부주의하여 개인정보가 노출되거나, 또는 홈페이지 이용자가 민원을 작성하거나 예약확인 요청 등을 위해 자신의 개인정보를 공개하여 개인정보가 노출되는 경우에 발생할 수 있습니다.

이렇듯 개인정보 노출을 발생시키는 주체에 따라 개인정보 취급자가 작성한 첨부파일 등을 통해 개인정보 노출이 발생하는 경우에는 개인정보 취급자 부주의, 홈페이지 이용자가 작성한 게시글 등을 통해 개인정보 노출이 발생하는 경우에는 홈페이지 이용자 부주의로 구분할 수 있습니다.

또한 홈페이지 설계 및 구현이 잘못된 경우 또는 홈페이지의 서버의 설정이 잘못되어 개인정보가 노출되는 경우를 홈페이지 설계 및 관리 미흡으로 구분할 수 있습니다.

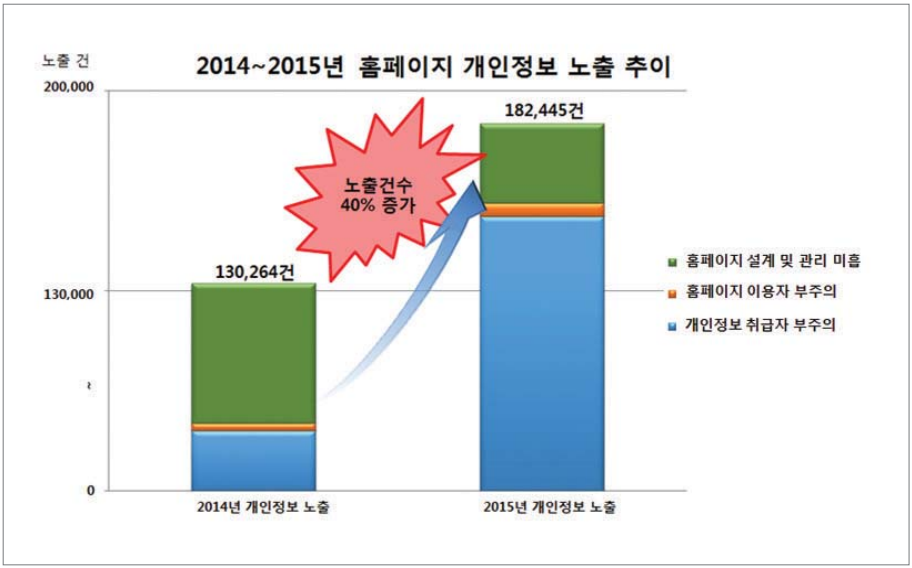
[표 2] 개인정보 노출의 원인

노출 원인	내 용
홈페이지 설계 및 관리 미흡	소스코드, URL, 홈페이지 취약점 등에 의해 개인정보가 노출되는 경우
첨부파일 노출	홈페이지에 개인정보가 포함된 첨부파일을 업로드 하는 경우
게시글 노출	홈페이지에 작성한 공지사항 및 댓글 등에 개인정보가 포함되어 있는 경우

[그림 2] 홈페이지 게시글 등록 시 개인정보 노출

개인정보 노출 현황을 분석해 보면,

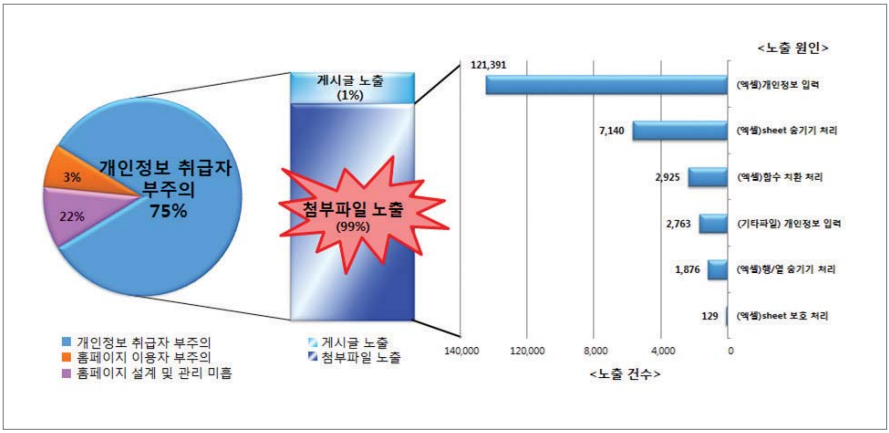
2015년에 홈페이지를 통한 개인정보 노출 건이 2014년 대비 약 40%(약 5만 건) 상승한 것을 볼 수 있습니다. [그림 3]에서 볼 수 있듯이 홈페이지 설계 및 관리 미흡은 지속적으로 감소되는 반면에, 파란색으로 표시된 개인정보 취급자 부주의로 인한 노출은 큰 폭으로 증가하고 있습니다.



[그림 3] 2014년~2015년 홈페이지 개인정보 노출추이

개인정보 노출 유형을 분석해 보면,

[그림 4]에서 볼 수 있듯이 개인정보 취급자 부주의로 인한 노출 건수가 전체의 75%를 차지하고 있습니다. 특히, 개인정보 취급자의 부주의로 인한 노출의 대부분이 개인정보가 포함된 첨부파일에 의해 발생하므로, 개인정보 취급자는 첨부파일을 등록하기 전에 해당 첨부파일 내에 개인정보가 포함되어 있는지 반드시 확인할 필요가 있습니다.



[그림 4] 2015년 개인정보 노출 원인 상세 분석한 노출 유형

[표 3] 공공/민간기관 주요 개인정보 노출 형태

대분류	중분류	주요 노출 형태	노출원인
공공기관	중앙행정기관	·참여마당 '자유게시판' 글에서 주민등록번호 노출 ·정보조회의 '일반정보' 글에서 운전면허번호 노출	게시글 노출
		·합격자발표 게시판의 'OO시험 합격자 명단' 첨부파일에서 여권번호 노출 ·임대안내 게시판의 신청서류 첨부파일에서 주민등록번호 노출 ·시험공고/공지사항 게시판의 '공채 임용유예자 명단' 첨부파일에서 주민등록번호 노출	첨부파일 노출
	지방자치단체	· '개별공시지가 이의신청' 첨부파일에서 주민등록번호 노출 ·과제검색 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출	첨부파일 노출
		·정보공개창 게시판의 '배출업소현황' 첨부파일에서 주민등록번호 노출 ·우리동소식 게시판의 '알선대상자 명단' 첨부파일에서 주민등록번호 노출 · 'OO시 선수명단' 파일에서 주민등록번호 노출 ·행정처분 명령서 파일에서 주민등록번호 노출	첨부파일 노출
	초중고	· '급식행정공개' , '가정통신문' 에서 주민등록번호 노출 ·행정실 게시판의 '운영위원회' 파일에서 주민등록번호 노출 ·부별업무자료의 '스카우트' 알집파일 내에 존재하는 첨부파일에서 주민등록번호 노출	첨부파일 노출
	대학교	·민원센터의 '학사/학적변동' 글에서 주민등록번호 노출 ·사이버강좌의 '개설강좌' 글에서 주민등록번호 노출	게시글 노출
		· '어학원 수강신청' 파일에서 외국인등록번호 노출 ·행정실 공지사항 게시판의 첨부파일에서 주민등록번호와 외국인등록번호 노출	첨부파일 노출
		·OO대학교 관리자페이지에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
민간기관	여행업	· '여행예약확인 요청' 글에서 주민등록번호, 여권번호 노출 · '현금 영수증 요청' 글에서 주민등록번호 노출	게시글 노출
		·고객센터의 '질문과 답변' 글에서 주민등록번호 노출 ·이용안내의 '자주 묻는 질문 FAQ' 글에서 주민등록번호 노출	게시글 노출
	의료업	·건강상담의 '복약상담' 글에서 주민등록번호 노출	게시글 노출
		·정보광장의 '채용공고' 파일에서 주민등록번호 노출 ·요양급여비용 청구서 파일에서 주민등록번호 노출	첨부파일 노출
		·건강진단 결과표에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
	협회	· '개인성적기록' 조회 게시판에서 주민등록번호 노출 · '참가팀 소개' 게시판에서 주민등록번호 노출	홈페이지 설계 및 관리 미흡
		· '자원봉사신청서' 첨부파일에서 주민등록번호 노출 ·내용 증명서 파일에서 주민등록번호 노출	첨부파일 노출
	단체	·본회소개의 '회원명단' 글에서 주민등록번호 노출	게시글 노출
		·자료실 게시판의 '경매실적' 첨부파일에서 주민등록번호와 외국인등록번호 노출 ·재단소개의 '정관/이사회' 첨부파일에서 주민등록번호 노출	첨부파일 노출

홈페이지 노출 유형별 조치방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법

- 가. URL(홈페이지 주소)에 개인정보 사용부분 삭제
- 나. 홈페이지 소스코드 내에 개인정보 삭제
- 다. 임시 저장 페이지의 올바른 처리 방법
- 라. 디렉터리 리스팅의 올바른 설정 방법
- 마. 관리자페이지의 올바른 구성 방법

2. 첨부파일이 포함된 게시글 노출 시 조치방법

- 가. 일반적인(HWP, DOC, XLS 등) 첨부파일인 경우
- 나. 이미지 형식(이미지형 PDF, 이미지파일 등)의 첨부파일인 경우

3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법

4. 검색엔진에 저장된 페이지 삭제 방법 공통사항

- 가. 개인정보가 노출된 페이지 또는 파일 검색
- 나. 개인정보가 있는 검색엔진 캐시페이지 삭제요청
  - 구글(Google)에 노출된 개인정보 삭제 방법
  - 네이버(Naver)에 노출된 개인정보 삭제 방법
  - 다음(Daum)에 노출된 개인정보 삭제 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출

홈페이지 설계 및 관리 미흡으로 인한 노출은 홈페이지 설계 당시 개인정보보호에 대해 충분히 고려하지 않고 홈페이지를 구축하여 개인정보가 노출되거나, 비공개 페이지에 대한 접근 제한이 미흡해 인증우회를 통해 개인정보가 노출되는 경우입니다.

[표 4] 홈페이지 설계 및 관리 미흡으로 인한 노출 유형

노출 유형	내 용
설계 미흡	URL에 개인정보가 노출
	이용자 화면 소스코드에 개인정보가 노출
	게시글 작성 중 임시 저장 페이지에 개인정보가 노출
	디렉터리 리스팅의 잘못된 설정으로 인해 개인정보가 노출
관리 미흡	관리자페이지 접근제한 미흡으로 인해 개인정보가 노출

가. URL에 개인정보가 노출된 사례

홈페이지 내의 특정페이지 주소(URL) 식별자로 주민등록번호 등을 사용하여 개인정보가 노출된 경우입니다.

주민등록번호는 개인을 구분하는 식별자로 사용할 수 없습니다. 홈페이지의 설계 변경을 통해 개인을 식별하는 값으로 별도의 구분자를 사용하고, 웹브라우저 주소 표시줄에 접속 파라미터가 나타나지 않도록 하는 것이 좋습니다.

[그림 5] URL에 주민등록번호가 노출된 사례

나. 이용자 화면 소스코드에 개인정보가 노출된 사례

홈페이지 화면상으로는 게시글에 개인정보가 포함되어 있지 않지만, 해당 화면에서 마우스 오른쪽 클릭 후 [소스보기]를 하면 글을 작성한 사람의 개인정보 확인이 가능한 경우입니다.

[그림 6]에서와 같이 게시글 화면 상에는 제목, 이름, 내용만 보이지만, 오른쪽 마우스 클릭 후 소스보기를 하면 소스코드 내에 개인정보가 포함되어 있는 것을 확인 할 수 있습니다.

개인정보가 이용자의 화면 상에는 보이지 않더라도 소스코드 상에 존재할 경우 개인정보가 노출되므로 홈페이지 설계 및 관리 시 이에 대한 조치가 반드시 필요합니다.

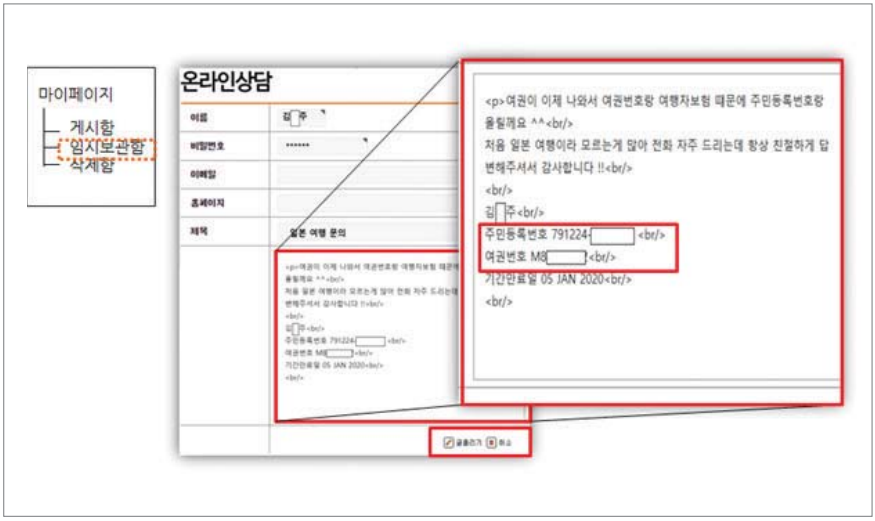
[그림 6] 소스보기에서 개인정보가 노출된 사례

다. 게시글 작성 중 임시 저장 페이지에 개인정보가 노출된 사례

홈페이지 설계 및 관리 미흡으로 인해 게시글의 임시 저장 페이지가 웹서버에 남아있어 해당 페이지의 개인정보가 노출된 경우입니다.

[그림 7]은 홈페이지 이용자가 여행사 홈페이지에 온라인상담 글을 작성하며 여행사에 제공할 개인정보 자료를 저장 완료하지 않고 임시 저장하여, 여행사 웹서버에 임시 저장 페이지가 남아있어 개인정보가 노출된 경우입니다.

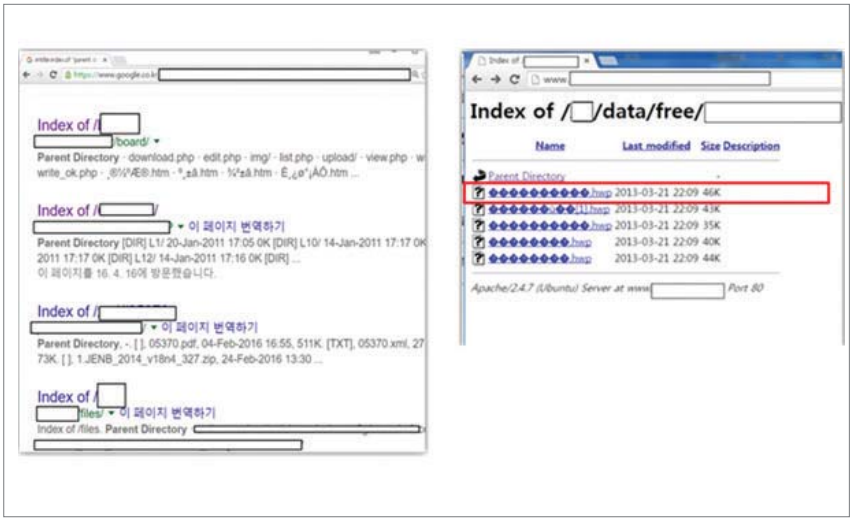
이러한 문제를 개선하기 위해 이용자가 홈페이지 접속을 종료하거나 게시글을 임시 저장한 후 일정기간이 지나면 임시 저장 페이지의 내용을 삭제하는 것이 좋습니다.



[그림 7] 임시보관함에 저장된 게시글 노출 사례

라. 디렉터리 리스팅의 잘못된 설정으로 인해 개인정보가 노출된 사례

디렉터리 리스팅 취약점은 개인정보의 노출 뿐 아니라 홈페이지 소스코드 전체가 노출되어 외부에 의한 해킹 등 2차적인 피해가 발생할 수 있고, 또 외부 검색엔진이 웹서버 디렉터리의 모든 파일들을 수집해 갈 수 있기 때문에 대량의 개인정보 노출이 발생할 수 있습니다.



[그림 8] 디렉터리 리스팅 취약점으로 개인정보가 노출된 사례

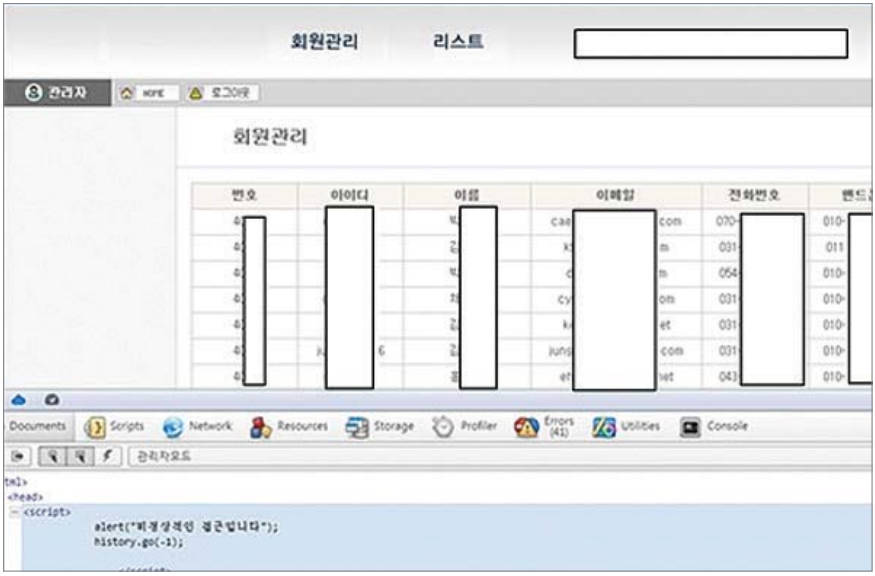
홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치방법 (예시)

Step 1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법(Ⅲ.1 참조)
Step 2. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)

마. 관리자페이지 접근제한 미흡으로 개인정보가 노출된 사례

관리자페이지에 인증절차를 마련하지 않아 누구나 접근할 수 있도록 방치되어 개인정보가 노출되는 사례입니다. 관리자페이지는 홈페이지 가입회원 정보를 모두 볼 수 있는 페이지가 존재하기 때문에, 일반적인 노출 사례보다 더 많은 개인정보가 노출될 수 있습니다.

관리자페이지는 내부 네크워크에서만 접근할 수 있도록 접근 권한을 제한하는 것이 좋습니다. 불가피하게 외부에서의 접근이 필요할 경우에는 IP접근제어 또는 VPN 등을 이용하는 것이 좋습니다.



[그림 9] 관리자페이지 접근제한 미흡으로 노출된 사례

2. 첨부파일에 의한 노출

게시판에 첨부되는 엑셀, 한글문서, PDF, 텍스트파일 등 다양한 유형의 첨부파일에 개인정보가 노출되는 경우를 말합니다. 개인정보 취급자가 공지사항 등 게시판에 첨부파일을 업로드 하면서 첨부파일 내에 개인정보 포함여부를 확인하지 않고 게시할 경우 발생됩니다.

첨부파일 중에서도 엑셀(Excel) 파일은 정보를 많이 저장할 수 있는 이점이 있지만, 한번 노출이 되었을 때 대량의 개인정보가 노출되는 위험이 있습니다.

엑셀 파일로 인한 노출 사례를 살펴보면 엑셀 내 개인정보 입력, Sheet 숨기기, 함수 치환, 행/열 숨기기, Sheet 보호, 글자색을 배경색과 동일하게 작성, 메모 내 개인정보 입력 등의 순으로 개인정보 노출 빈도가 나타나며, 매우 다양한 유형으로 개인정보가 노출 되고 있음을 알 수 있습니다.

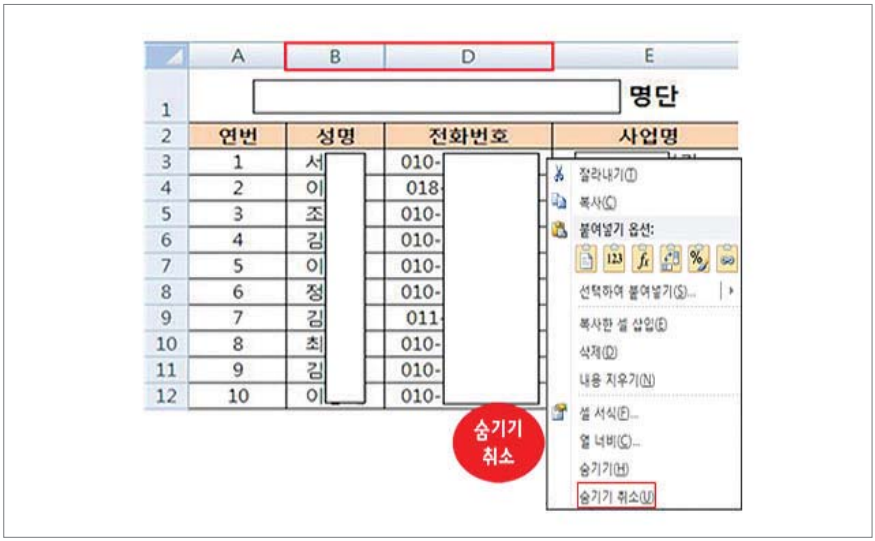
첨부파일로 인한 노출 대부분은 개인정보 취급자가 의도적으로 개인정보를 감추고자 한 목적이기 보다는 첨부파일 내 개인정보 포함 유무를 제대로 확인하지 않고 업로드하여 문제가 발생하는 경우가 많습니다.

[표 5] 엑셀 및 이미지 파일에 의한 노출 유형

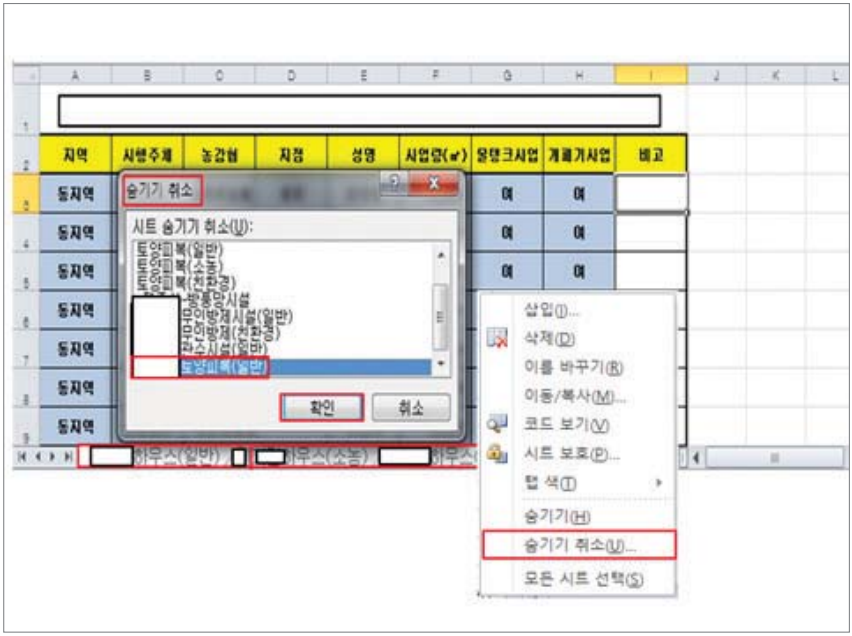
노출 유형	내 용
엑셀파일에 의한 노출	[숨기기] 기능에 의한 개인정보 노출
	시트보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보 노출
	함수 치환 후 원본 내용 미삭제로 인한 개인정보 노출
	[메모]기능으로 인한 개인정보 노출
	배경색과 같은 글자색으로 작성하여 개인정보 노출
	OLE 객체로 인한 개인정보 노출
이미지파일에 의한 노출	개인정보가 담긴 이미지형 PDF 파일에 의한 노출
	개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의한 노출

가. [숨기기] 기능에 의해 개인정보가 노출된 사례

개인정보 취급자가 엑셀 파일에서 행/열 또는 Sheet [숨기기] 처리된 것을 확인 하지 못하여 개인정보 노출이 발생하는 경우입니다. 엑셀파일에는 행/열 또는 Sheet [숨기기] 기능이 있습니다. 개인정보가 포함된 행/열 또는 Sheet를 [숨기기] 처리한 파일을 열었을 때에는 개인정보가 바로 보이지는 않지만 행/열 또는 Sheet [숨기기 취소]를 할 경우 개인정보가 고스란히 포함된 것을 알 수 있습니다.



[그림 10] 열 숨기기 기능으로 개인정보 저장여부 미확인



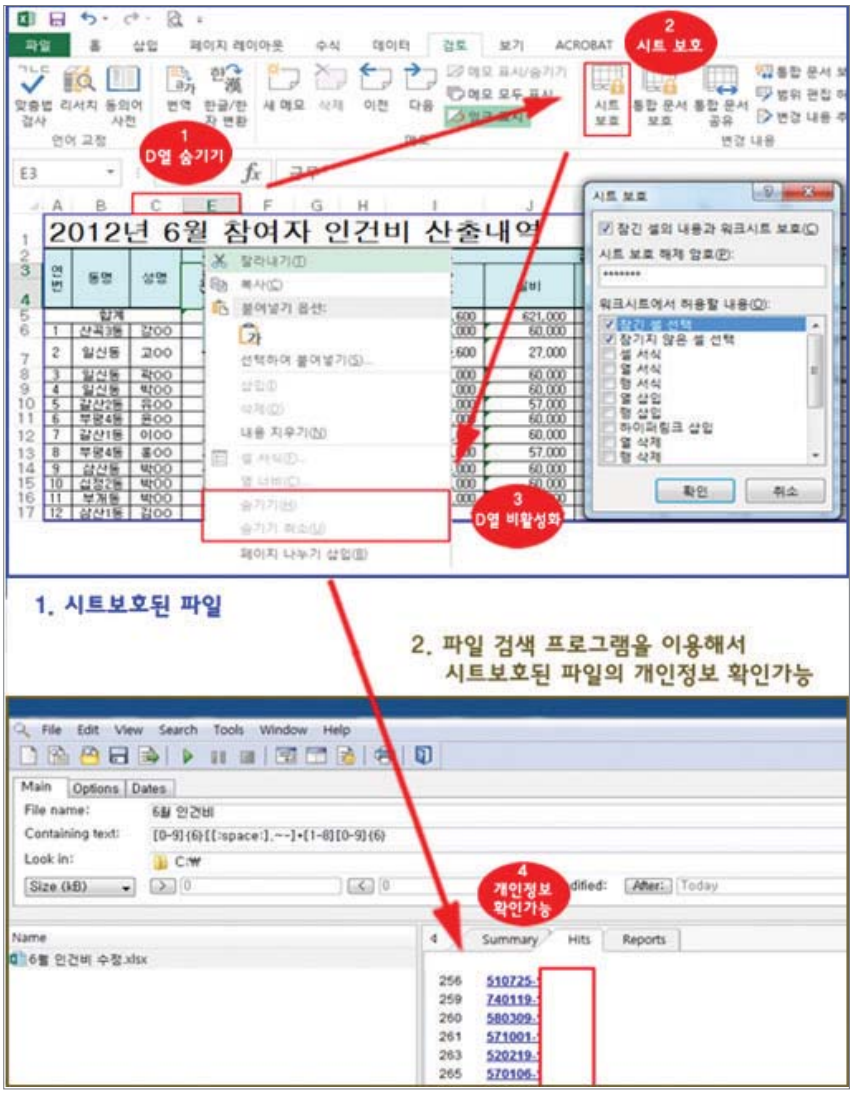
[그림 11] 시트 숨기기 기능으로 개인정보 저장여부 미확인

나. 시트보호 기능으로 내용을 볼 수 없다고 오인하여 개인정보가 노출된 사례

개인정보 취급자가 엑셀의 시트보호 기능을 잘 못 활용하여 개인정보 노출이 발생하는 경우입니다. 엑셀의 시트보호 기능은 데이터를 암호화하는 기능이 아니라, 데이터가 변경되지 않도록 보호하는 기능입니다.

즉 숨기기 기능을 이용해 개인정보를 보이지 않도록 한 후 시트보호 기능으로 암호를 설정하더라도 숨겨진 데이터는 암호화되지 않아 개인정보 검색 시 노출되므로 주의해야 합니다.

따라서 파일검색 시 내용 확인이 되지 않도록 하려면 엑셀에서 제공하는 파일 암호설정 기능을 사용해야 합니다.



[그림 12] 시트보호로 개인정보가 보호되지 않는 사례

다. 함수 치환 후 원본 내용 포함으로 인해 개인정보가 노출된 사례

개인정보 취급자가 엑셀파일에서 개인정보가 포함된 셀을 LEFT나 REPLACE 등의 함수를 이용하여 주민등록번호 뒷자리를 *******(마스킹 처리) 하였으나 원본 자료가 삭제되지 않고 남아있어 개인정보가 노출된 경우입니다.

[그림 13]과 같이 함수 치환 기능을 사용하여 개인정보를 마스킹 처리하였지만, 마스킹 처리를 위한 원본 자료가 함께 존재하므로 함수 치환 기능으로는 개인정보를 보호할 수 없습니다.

따라서, 함수 치환 후에는 원본 자료를 반드시 삭제해야 합니다.

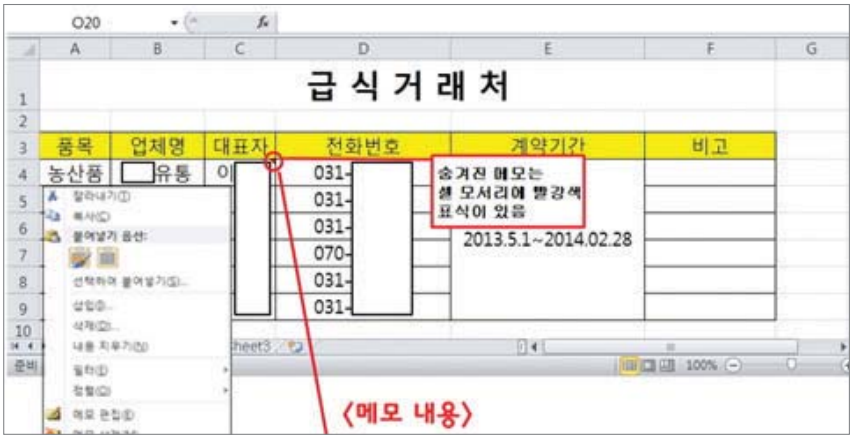
[그림 13] 함수 치환 후 원본자료 포함으로 인한 노출사례

라. [메모]기능에 포함된 개인정보 미삭제 사례

엑셀파일의 [메모] 기능 이용 시 메모 내용에 개인정보가 포함되어 개인정보 노출이 발생하는 경우입니다.

[그림 14]는 급식 거래처 명단에서 업무편의상 [메모] 기능을 사용하여 대표자 주민등록번호를 기록한 후, 메모 숨기기 기능으로 화면 상에 보이지 않게만 처리하여 개인정보가 노출된 사례입니다.

숨겨진 메모는 메모 숨기기 취소 기능을 통해 언제든지 내용을 다시 확인할 수 있으므로 개인정보가 포함되어 있을 경우 완벽하게 삭제하는 것이 좋습니다.



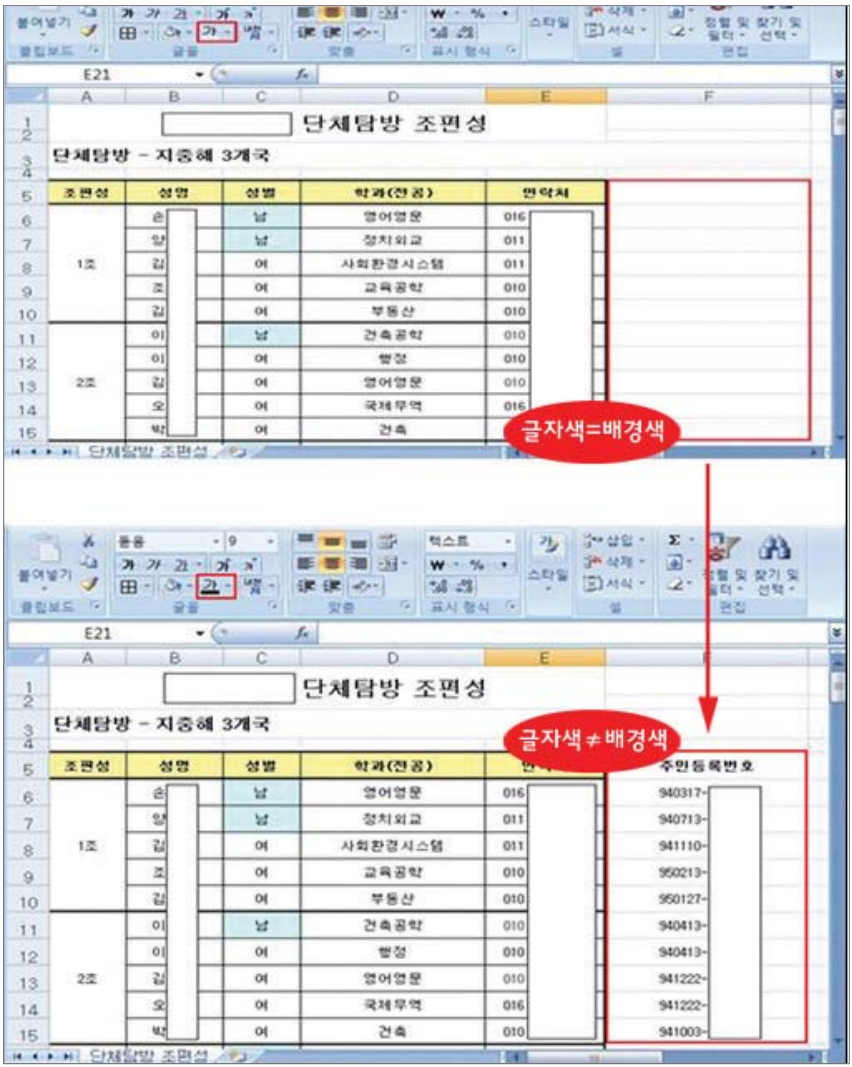
[그림 14] [메모] 내용에 개인정보가 포함된 사례

마. 배경색과 같은 글자색으로 작성하여 개인정보가 노출된 사례

파일 내 개인정보의 글자색과 배경색이 같아서 개인정보가 없는 것처럼 보이는 경우입니다. 육안으로는 보이지 않지만, 검색이나 드래그를 통해 없는 것처럼 보이는 글자들을 확인할 수 있습니다.

[그림 15]는 주민등록번호를 배경색과 같은 글자색(흰색)으로 작성하여, 웹사이트 이용자의 눈으로는 바로 확인할 수 없었으나, 개인정보 검색 프로그램을 통해서는 쉽게 찾아낼 수 있었던 사례입니다.

개인정보를 보이지 않게만 처리하는 것은 안전한 조치가 아닙니다. 개인정보를 식별하지 못하도록 마스킹 처리하거나 불필요한 개인정보는 삭제하는 것이 좋습니다.



[그림 15] 배경색과 같은 색상으로 글자색을 지정하여 개인정보 노출된 사례

바. OLE 객체로 인해 개인정보가 노출된 사례

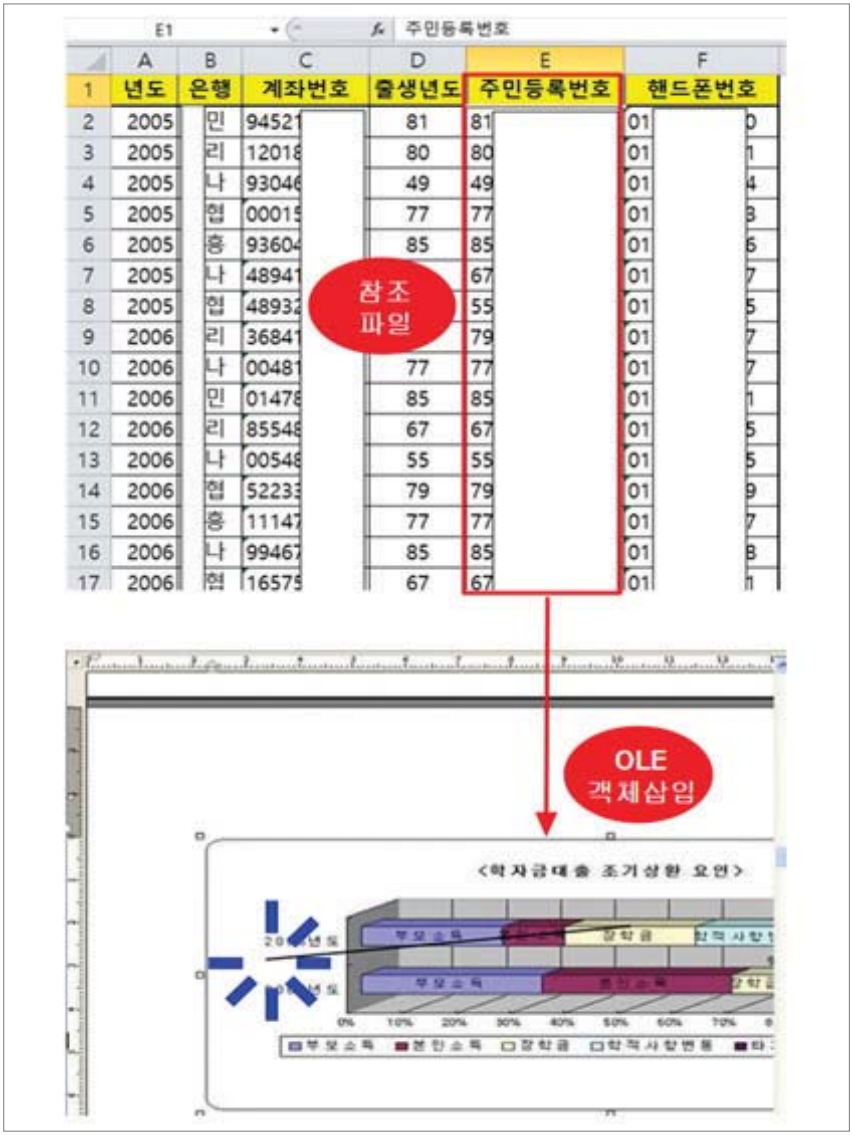
개인정보가 포함된 엑셀파일을 OLE(Object Linking and Embedding) 객체로 삽입한 후 해당 자료를 홈페이지에 게시하여 개인정보 노출이 발생하는 경우입니다.

[그림 16]과 같이 OLE 객체가 삽입되어 있는 그래프를 더블클릭하면 참조되어 있던 자료가 표시되는데, 그래프 상에 표시되지 않더라도 개인정보가 참조된 자료 내에 존재할 경우 무방비로 노출이 됩니다. 따라서 OLE 객체를 삽입할 때는 참조 파일 내에 나타내고자 하는 항목만 추려 작성해야만 합니다.

업무용 파일을 OLE객체와 연결할 경우 개인정보 등 원하지 않는 항목까지 포함 될 수 있으므로 반드시 주의가 필요합니다.

첨부파일에 의한 노출 시 조치방법 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 첨부파일이 포함된 게시글 노출 시 조치 방법(Ⅲ.2 참조)
Step 3. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)



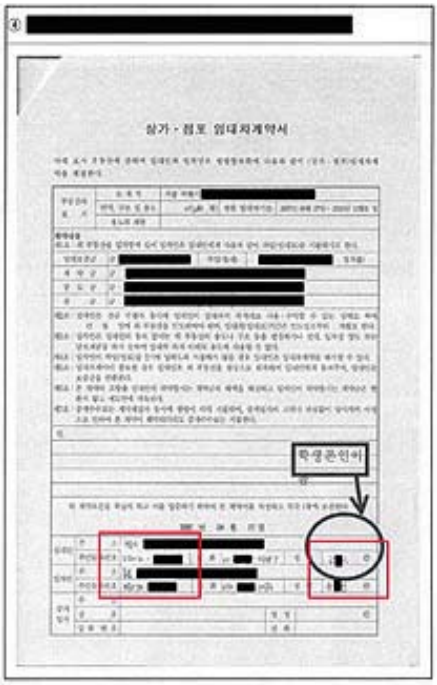
[그림 16] OLE 객체 내에 있는 개인정보 노출 사례

사. 개인정보가 담긴 이미지형 PDF 파일에 의해 노출된 사례

개인정보가 이미지형 PDF 파일에 포함되어 노출된 사례입니다.

일반 PDF 파일은 텍스트 기반으로 단어검색이 가능하여 첨부파일을 등록하기 전에 개인정보를 점검하는 것이 용이하지만, 이미지형 PDF 파일은 이미지를 PDF 형태로 저장하기 때문에 텍스트 검색 기능을 사용하기 어렵습니다.

따라서, 스캐너 등으로 생성된 이미지형 PDF 파일을 홈페이지에 등록할 경우에는 개인정보가 포함되어 있는지 육안으로 확인하는 것이 좋습니다.

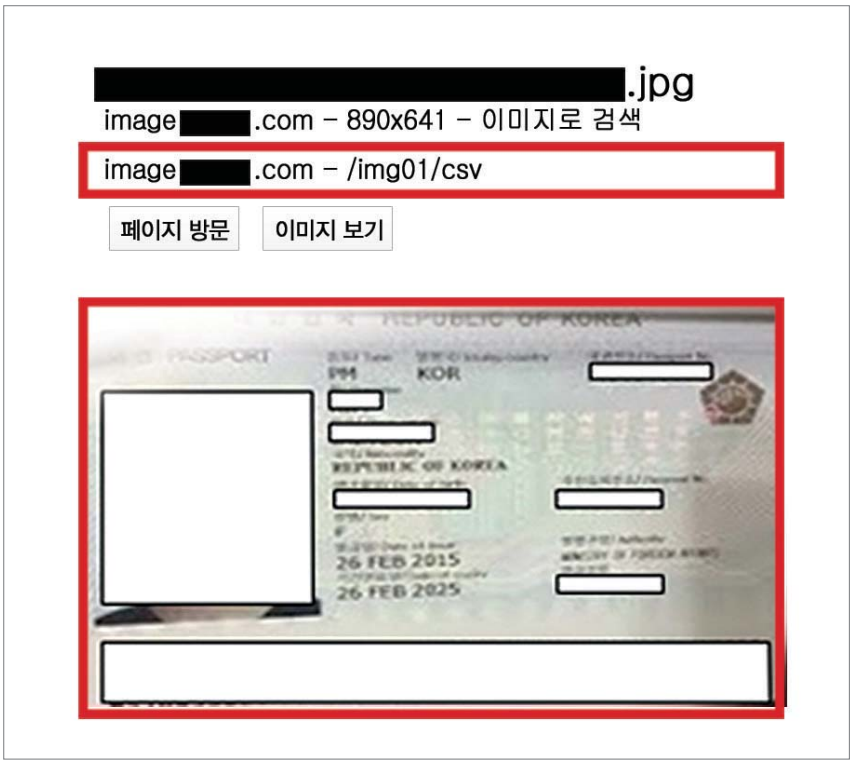


[그림 17] 이미지형 PDF 파일에 의한 노출 사례

아. 개인정보가 담긴 이미지 파일(JPG, GIF, BMP, PNG 등)에 의해 노출된 사례

개인정보가 이미지 파일(JPG, GIF, BMP, PNG 등)에 포함되어 노출된 사례입니다.

[그림 18]은 여행자보험 신청을 위해 여권사본을 여행사 홈페이지에 등록하였으나 디렉터리 리스팅 취약점에 의해 개인정보가 노출된 사례입니다. 개인정보가 포함된 이미지 파일의 노출을 방지하려면 디렉터리 리스팅 취약점 개선 및 개인정보가 포함된 이미지의 마스킹 처리가 필요합니다.



[그림 18] 웹서버에 저장된 여권사본 이미지 파일에 의한 개인정보 노출 사례

3. 게시글에 의한 노출

게시판을 통한 개인정보 노출 원인은 크게 두 가지 입니다. 첫째는 게시판에 게시글(공지사항, 민원 등)을 작성하면서 주민등록번호, 휴대폰번호 등이 포함되어 개인정보가 노출되는 경우이며, 둘째는 게시글에 대한 댓글을 작성하면서 개인정보가 노출되는 경우입니다.

[표 6] 게시글에 의한 노출 유형

노출 유형	내 용
게시글 노출	홈페이지 공지사항 등 게시글을 작성 시 개인정보가 포함 됨
댓글 노출	게시글에 대한 댓글을 작성 시 개인정보가 포함 됨

가. 게시글 작성에 의한 노출 사례

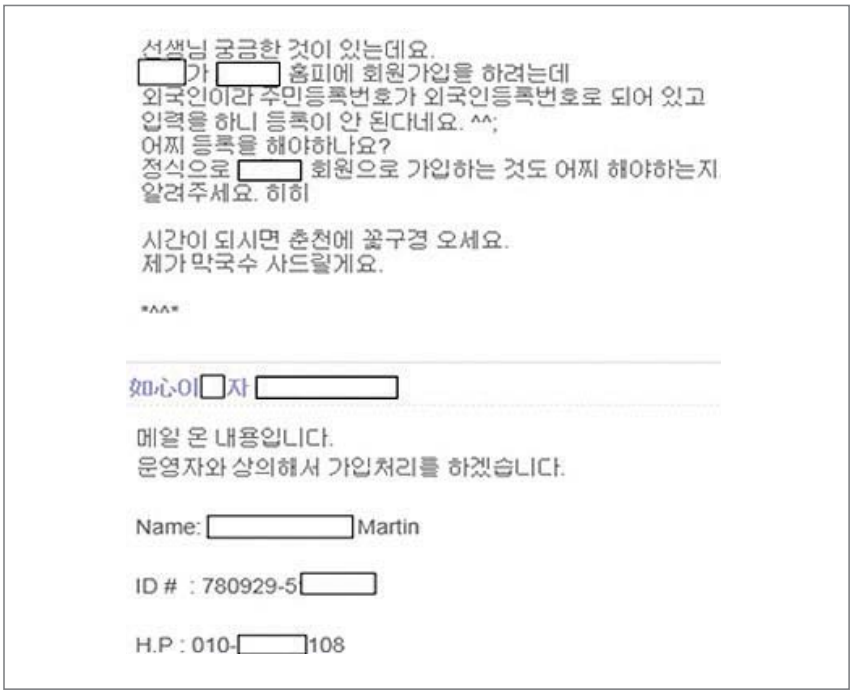
공지사항 등의 게시글 작성 시, 개인정보 취급자 및 홈페이지 이용자의 부주의로 게시글에 개인정보가 포함되어 노출되는 경우입니다.

[그림 19]는 홈페이지 이용자가 대학교 재학 중 취득한 자격증의 재발급을 요청하면서 본인의 연락처가 게시글에 노출되었던 사례입니다. 이 경우 홈페이지 이용자는 개인정보 부분과 연락처에 대해 **** 등으로 마스킹 처리를 하거나 해당 게시글을 비밀글로 전환하는 것이 필요합니다.

[그림 19] 홈페이지 이용자의 게시글에 개인정보가 노출된 사례

나. 댓글 작성에 의한 노출 사례

[그림 20]은 개인정보 취급자가 홈페이지 이용자의 요청사항에 대한 답변을 작성하면서 홈페이지 이용자의 개인정보가 노출되었던 사례로 개인정보 취급자의 상당한 주의가 필요한 경우입니다.

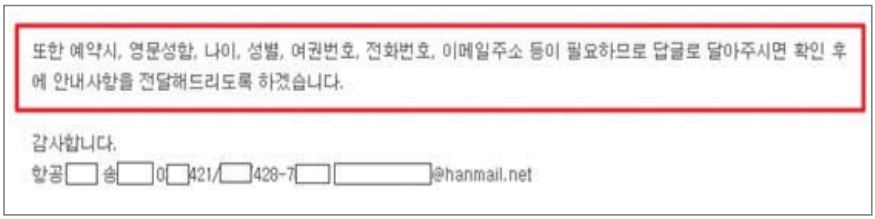


[그림 20] 개인정보취급자의 댓글에 개인정보가 노출된 사례

[그림 21]은 여행사에서 예약 업무처리를 목적으로 공개된 게시글에 개인정보 입력을 유도한 사례입니다.

개인정보 취급자는 업무편의를 위하여 홈페이지 이용자의 개인정보를 게시글에 공개적으로 작성하도록 유도해서는 안 됩니다. 업무처리를 위한 게시글은 홈페이지 이용자와 개인정보 취급자만 볼 수 있도록 비밀글로 처리하는 것이 좋습니다.

이 경우 개인정보 작성을 유도하는 안내글을 삭제하고, 공개된 게시글에 등록된 개인정보는 **** 등으로 마스킹 처리하거나 삭제해야만 합니다.



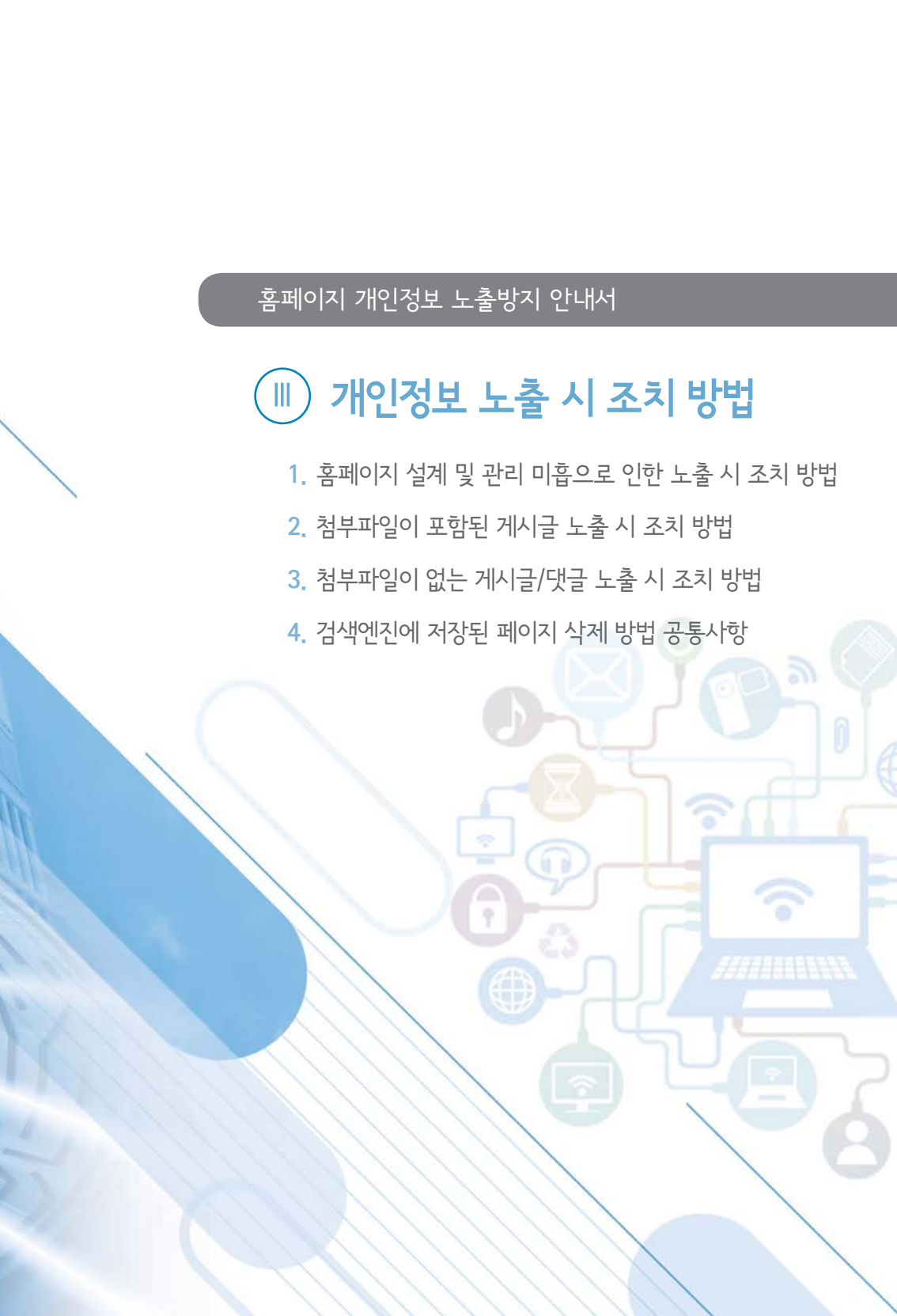
[그림 21] 빠른 업무처리를 위해 개인정보 노출을 유도한 사례

게시글/댓글 노출 시 조치방법 (예시)

Step 1. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법(Ⅲ.3 참조)
Step 2. 검색엔진에 저장된 페이지 삭제 방법(공통사항)(Ⅲ.4 참조)

Ⅲ 개인정보 노출 시 조치 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법
2. 첨부파일이 포함된 게시글 노출 시 조치 방법
3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법
4. 검색엔진에 저장된 페이지 삭제 방법 공통사항



Ⅲ 개인정보 노출 시 조치 방법

1. 홈페이지 설계 및 관리 미흡으로 인한 노출 시 조치 방법

가. URL(홈페이지주소)에 개인정보 사용부분 삭제

홈페이지 설계 시 구분하기 위한 값으로 개인정보를 사용하는 경우 URL에 개인정보가 노출됩니다. 조치 방법은 개인을 구분하기 위한 값으로 개인정보를 사용하지 않고, 웹브라우저 주소 표시줄에 파라미터 값이 보이지 않도록 GET 방식보다는 POST 방식을 사용하는 것입니다.

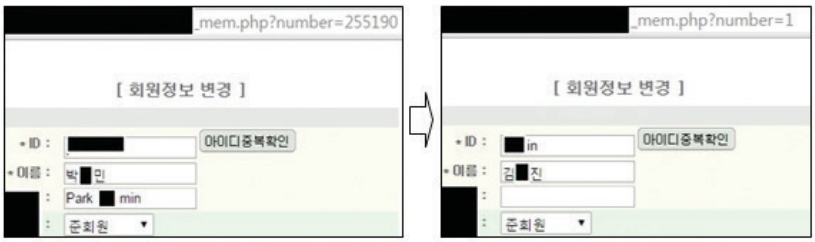
이 작업은 홈페이지의 프로그램 코드를 수정하는 것으로 개발 또는 운영 인력과 함께 처리해야 합니다.

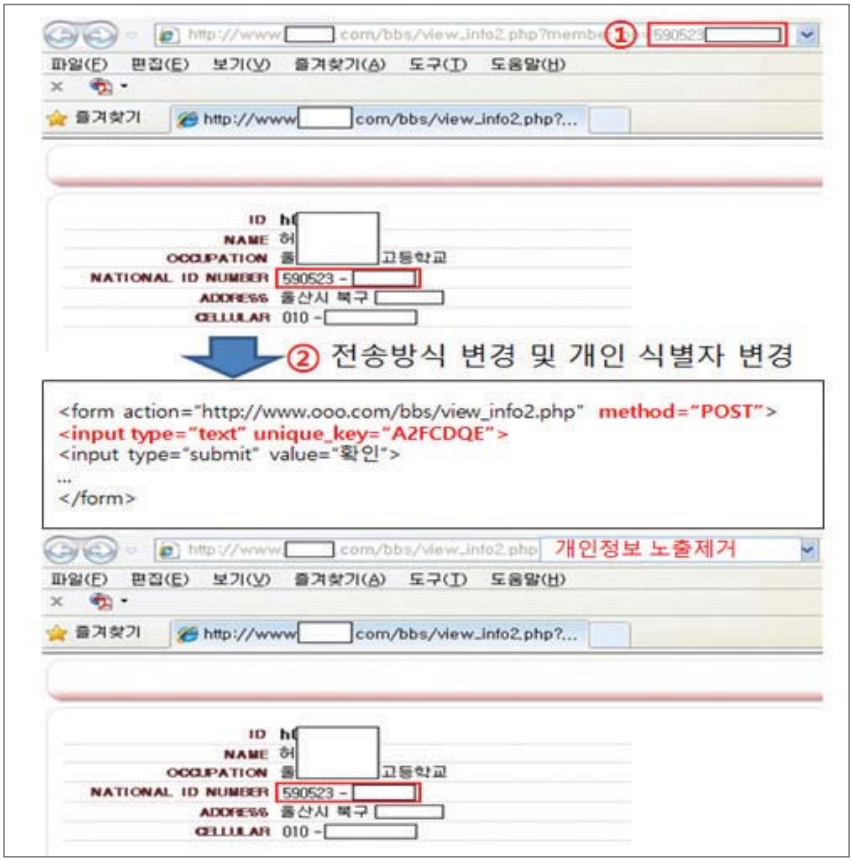
※ 홈페이지에서 개인 식별자의 변경은 많은 작업이 수반될 수 있으니 기술적인 부분에 대한 검토를 반드시 진행한 후 처리하도록 합니다.

참고사항

파라미터 값을 개인정보가 아닌 다른 값(숫자 등)으로 할당하는 경우에도, 하나의 파라미터를 습득 후 임의 변경을 통해 타인의 개인정보를 열람할 수 있습니다.

개인정보가 포함된 페이지는 인증절차를 마련하여 파라미터 임의 변경을 통한 개인정보 노출을 예방하는 것이 좋습니다.





[그림 22] URL에 개인정보가 노출된 경우 조치방법

처리절차 (예시)

Step 1. URL에 개인정보 노출여부 확인
Step 2. URL에 개인을 구분할 수 있는 값 정의 후 홈페이지에 적용
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

나. 홈페이지 소스코드 내에 개인정보 삭제

홈페이지 설계 시 화면에서는 보이지 않지만 소스코드 내부에 개인정보가 포함된 경우가 있습니다. 이 경우 간단히 소스 보기를 통해 개인정보가 노출될 수 있습니다.

이에 대한 조치 방법은 개인을 구분하기 위한 값을 변경하는 것으로, 해당 작업은 홈페이지 설계부분에 대한 전반적인 검토가 필요하기 때문에 개발 또는 운영자와 함께 빠르게 조치해 나가야 합니다.

[그림 23] 홈페이지 소스코드 내에 개인정보가 노출된 경우 조치 방법

처리절차 (예시)

Step 1. 인터넷 브라우저에서 소스보기를 통해 개인정보가 있는지 확인
Step 2. 업무 처리 시 불필요한 개인정보는 프로그램에서 삭제하고 꼭 필요한 정보는 암호화 처리
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조))

다. 임시 저장 페이지의 올바른 처리 방법

임시 저장 페이지는 홈페이지 이용자의 편의를 위해 제공하는 기능입니다. 홈페이지 이용자가 작성 중인 게시글의 내용이 없어지지 않도록 그 내용을 임시로 저장하는 것이지만, 작성 중인 게시글을 작성 완료하거나 또는 작성을 취소했을 경우에는 웹서버에 있는 임시 저장 페이지를 반드시 삭제해야 합니다.

임시 저장 페이지에서 개인정보가 노출되지 않도록 하기 위해서는 게시글 작성 완료 및 작성 취소 시 저장된 임시 페이지를 바로 삭제하고, 일정기간이 경과된 임시저장 페이지는 자동으로 삭제될 수 있도록 조치하는 것이 좋습니다.

소상공인, 중소사업자 및 비영리단체 대상 개인정보 보호 기술 지원

구분	내 용
지원내용	· 개인정보 보호조치 컨설팅 · 홈페이지 웹 취약점 점검 서비스 · 업무용PC 점검도구 제공 · 주민등록번호 미 수집, 암호화 조치 지원
절차/방법	· 우편, FAX, 이메일, 홈페이지
온라인신청	· 개인정보보호 종합포털(www.privacy.go.kr) 〉 사업자 〉 개인정보보호 기술지원
문의처	· 한국인터넷진흥원 개인정보보호 기술지원센터 (☎ 118)

※ 본 내용은 참고사항이며 해당 여부는 서비스 신청 후 심사기관의 별도 조사를 통해 확인 바랍니다.

라. 디렉터리 리스팅의 올바른 설정 방법

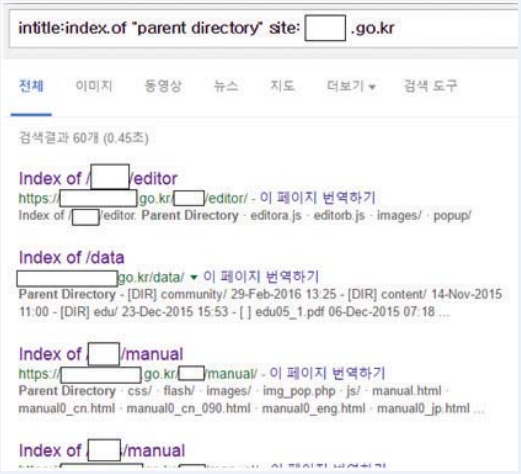
디렉터리 리스팅 설정은 웹브라우저를 이용한 자료 관리를 위해 주로 사용하지만 홈페이지의 모든 디렉터리를 볼 수 있어 보안성 면에서 취약한 서버설정입니다. 서버에 있는 모든 경로에 직접 접근이 가능하므로 회원 개인정보와 관련된 파일들이 외부로 노출될 수 있습니다.

디렉터리 리스팅 취약점이 발견될 경우, 웹 서버에서 해당 디렉터리를 외부에서 읽지 못하도록 디렉터리의 설정을 변경하여야 합니다.

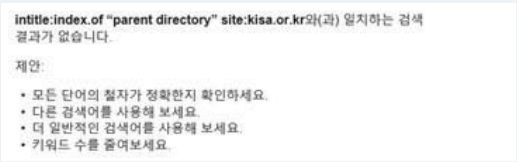
디렉터리 리스팅

서버관리자가 사이트 테스트 목적으로 사용하는 설정으로 브라우징하는 모든 디렉터리를 볼 수 있지만 그만큼 보안에 매우 취약한 서버설정입니다. 서버에 있는 모든 경로에 직접 접근이 가능하므로 회원 개인정보에 대한 파일이 외부로 노출될 수 있습니다.

☑ **디렉터리 리스팅 검색방법**



[그림 24] 디렉터리 리스팅 취약점이 있는 홈페이지의 검색 예시



[그림 25] 디렉터리 리스팅 취약점이 없는 홈페이지의 검색 예시

UNIX 또는 LINUX 환경

☑ Apache : httpd.conf 파일에서 indexes 문자열 제거

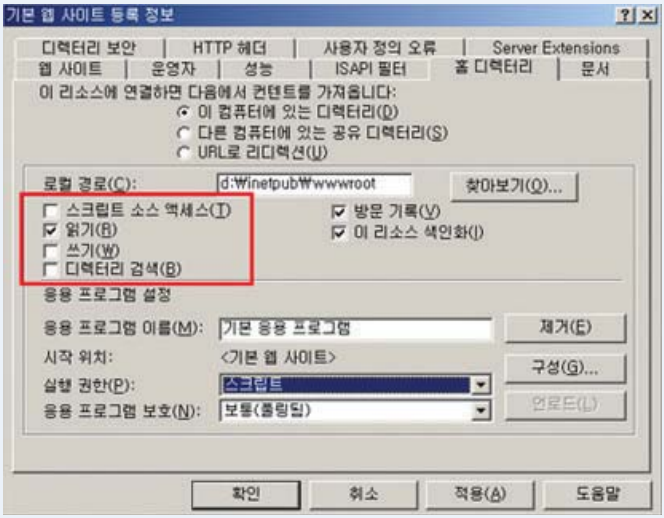
```
<Directory "/user/local/server/apache/htdocs">
        Options Indexes
</Directory>
```

☑ Tomcat : web.xml 파일에서 param-value false 로 설정변경

```
<init-param>
  <param-name>listings</param-name>
  <param-value>false</param-value>
</init-param>
```

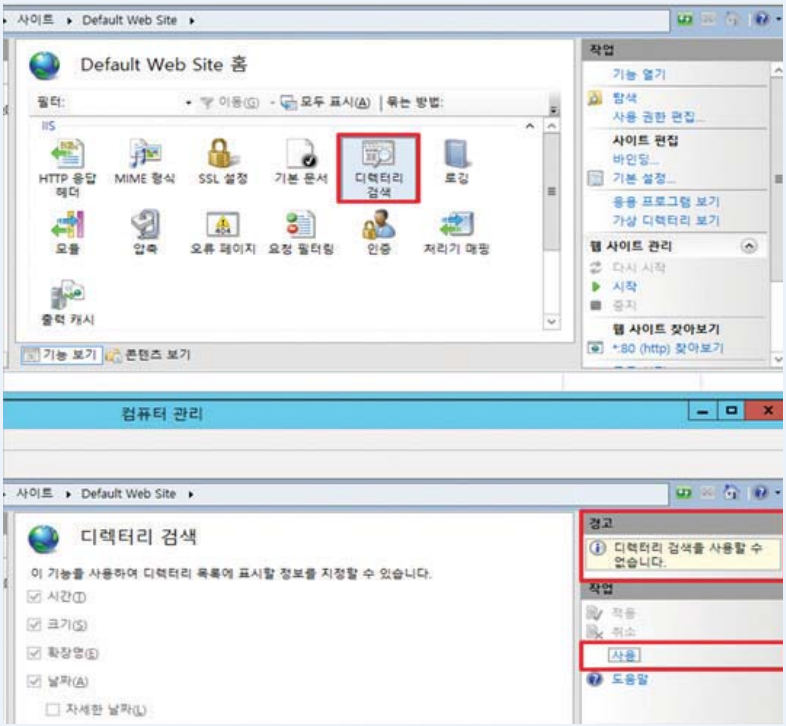
윈도우 IIS(Internet Information Service) 환경

☑ IIS 6.x 이하 : 제어판 → 관리도구 → 인터넷 서비스 관리자
→ 기본 홈페이지 의 속성에서디렉터리 검색 부분을 비활성화



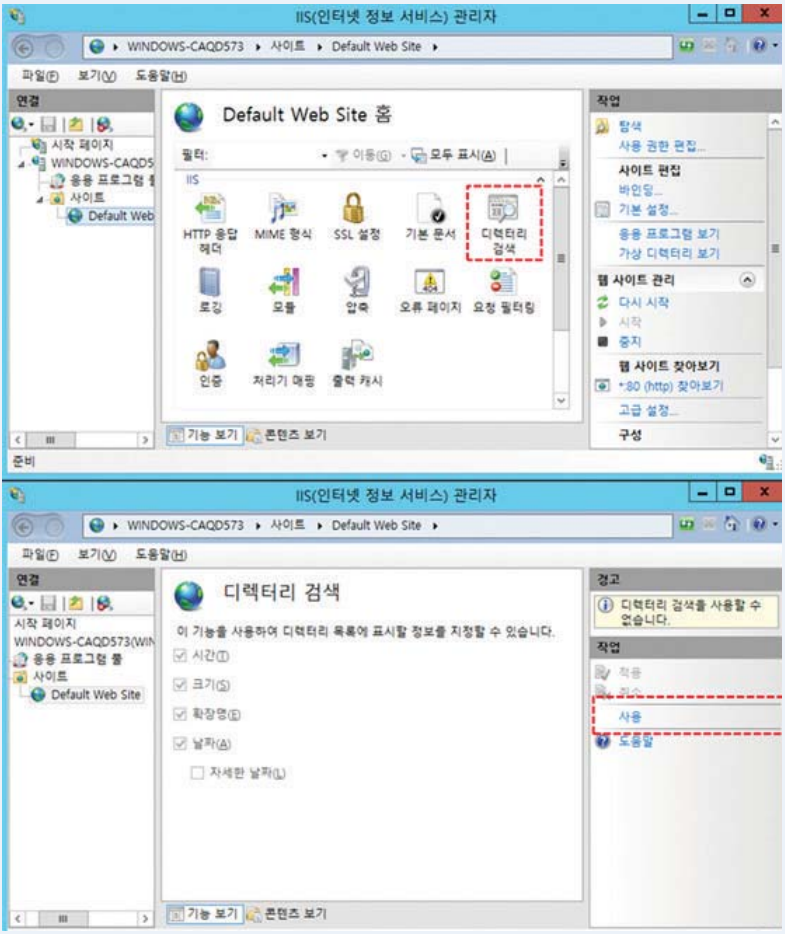
[그림 26] IIS 6.x 이하에서 디렉터리 리스팅 방지 설정

☑ IIS 7.x : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 홈페이지 홈 → 디렉터리 검색을 더블클릭 후 속성에서 우측 작업창에서 사용 해제



[그림 27] IIS 7.x 에서 디렉터리 리스팅 방지 설정

IIS 8.x : 제어판 → 시스템 및 보안 → 관리도구 → IIS(인터넷 정보서비스) 관리자 → 사이트 → 기본 홈페이지 홈 → 디렉터리 검색을 더블클릭 후 속성에서 우측 작업창에서 사용 해제



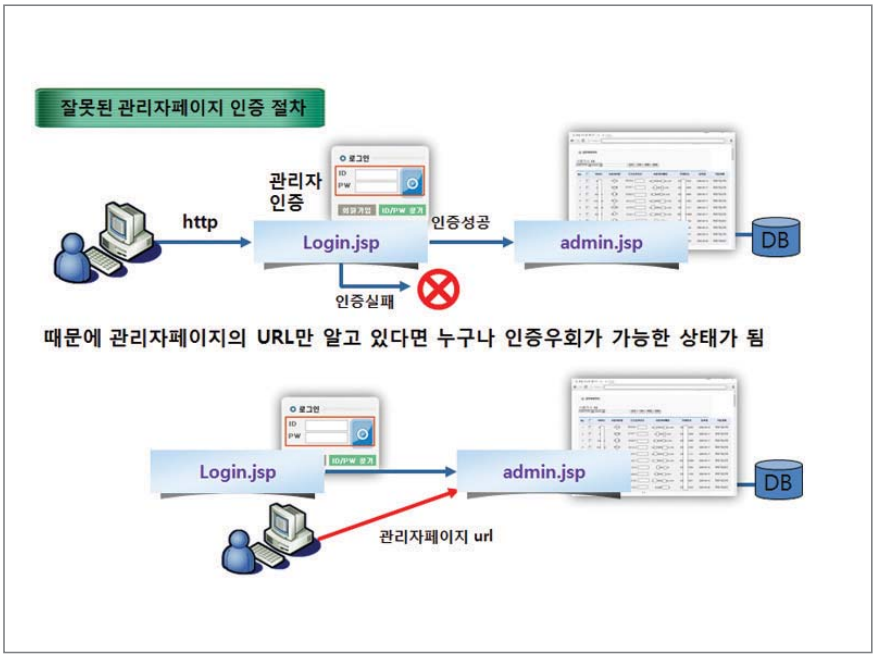
[그림 28] IIS 8.x 에서 디렉터리 리스팅 방지 설정

마. 관리자페이지의 올바른 구성 방법

관리자페이지의 접근권한 관리가 미흡한 경우 서비스 이용자들의 개인정보가 노출되어 해당 정보가 악용되는 피해가 발생할 수 있습니다. 홈페이지에 관리자페이지의 주소를 링크로 만들어서는 안 되며, 관리자페이지의 주소를 쉽게 추측 가능한 주소로 사용하지 말아야 합니다.

또한, 관리자페이지 접근을 위한 인증정보(세션 정보 등)는 처음 로그인화면 뿐 아니라 관리자페이지 전체에서도 모두 체크하도록 하여 제3자가 인증 없이 관리자페이지에 접근하는 것을 방지하도록 합니다.

마지막으로 관리자페이지를 외부에서 접속할 때는 전용선이나 가상사설망(VPN)을 이용하는 것이 좋습니다.



[그림 29] 관리자페이지 구성

외부 검색엔진의 이해

검색엔진은 인터넷에 공개된 홈페이지의 정보를 수집하여 홈페이지 이용자들이 원하는 정보를 쉽게 찾아주는 기능을 제공합니다. 검색엔진의 크롤러(수집기)는 인터넷의 홈페이지를 돌아다니며 정보를 수집하여 검색엔진 DB에 저장합니다. 이용자가 검색엔진에 (1) 질의어를 전달하면 (2) 검색엔진은 검색엔진 DB에서 질의어를 색인하여 (3) 검색결과를 이용자에게 전달합니다. 이 과정에서 다양한 정보가 검색엔진 DB에 수집되며 개인정보나 비공개 자료도 포함될 수 있습니다.

[그림 30] 검색엔진의 질의어 검색 과정

검색엔진에 수집되는 기관 홈페이지 내용 확인

일반적으로 공공기관은 홈페이지를 통해 기관 업무를 이용자들에게 서비스하거나, 정보를 제공하는 용도로 사용하고 있습니다. 홈페이지 이용자들은 자신이 필요로 하는 내용을 검색엔진을 통해 검색할 수 있습니다. 이처럼 기관 담당자들이 홈페이지에 게시하는 글이나 자료가 외부 검색엔진을 통해 검색될 수 있으므로, 검색엔진을 통해 수집되고 있는 기관 홈페이지의 내용을 파악하고 있어야 개인정보 노출을 예방할 수 있고, 노출 발생 시 신속히 개인정보가 포함된 자료를 검색하여 삭제조치 할 수 있습니다.

웹마스터 도구 사용방법 숙지

홈페이지에 개인정보가 포함된 자료가 게시되었다면 즉시 해당 자료를 삭제조치 해야 하며, 외부 검색엔진이 해당 자료를 수집해갔는지 확인해봐야 합니다. 이를 위해서는 국내/외 포털사이트 및 검색엔진에서 노출된 자료를 삭제하는 방법을 숙지해야 합니다(Ⅲ.4 참조).

검색엔진에 저장된 페이지

키워드 등을 사용하여 검색한 결과페이지에는 두가지 종류의 페이지가 있습니다. 하나는 현재 운영중인 페이지 정보이고, 다른 하나는 검색엔진이 이전에 수집하여 보관하고 있는 캐시된 페이지 정보입니다.

따라서, 개인정보 노출시 현재 페이지의 정보만 수정한다고 해서 노출이 차단되지 않으며, 캐시된 페이지까지 모두 삭제가 되어야 노출이 차단됩니다.

2. 첨부파일이 포함된 게시글 노출 시 조치 방법

첨부파일에 개인정보가 포함되어 노출되는 유형은 일반적인 문서파일(HWP, DOC, XLS, PPT 등)에 의한 노출과 이미지 형식의 파일에 의한 노출로 구분할 수 있습니다. 첨부파일에 의한 노출 발생 시 일반 문서파일인지 이미지 형식의 파일인지 먼저 확인하고 조치를 취해야 합니다.

가. 일반적인(HWP, DOC, XLS 등) 첨부파일인 경우

첨부파일에 개인정보가 포함되어 노출된 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제한 후 첨부파일 내에 있는 개인정보를 삭제하거나 123456-1****** 와 같이 마스킹 처리하여 재등록 합니다. 또한, 웹서버에서 첨부파일이 저장되어 있는 디렉터리(예:/홈페이지/첨부파일폴더)를 찾아서 개인정보가 있는 파일을 반드시 삭제해야 합니다. 개인정보를 삭제 또는 마스킹 처리한 파일을 재등록 했어도 웹서버에는 기존 파일이 남아있어 외부에 지속적으로 노출될 수 있습니다.

[그림 31] 첨부파일 내 개인정보 노출 시 조치 절차

마지막으로, 노출된 페이지의 처리가 끝난 후에는 항상 검색엔진에서 해당 페이지가 수집되었는지 확인하고, 수집된 페이지가 있을 시 삭제요청을 하여야 합니다.

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 첨부파일의 개인정보 삭제 또는 123456-1******와 같이 마스킹 처리하여 재등록
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

나. 이미지 형식(이미지형 PDF, 이미지파일 등)의 첨부파일인 경우

이미지 형식(이미지형 PDF, JPG, PNG, TIF 등)의 첨부파일이 노출되었을 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제하거나, 이미지를 편집할 수 있는 소프트웨어(그림판 등)를 사용하여 개인정보 부분을 마스킹 처리 한 후 재등록하도록 합니다.

[그림 32] 이미지형 마스킹 처리 예시

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 이미지형 첨부파일의 삭제 또는 개인정보 부분 이미지를 지운 후 재등록(마스킹처리)
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

3. 첨부파일이 없는 게시글/댓글 노출 시 조치 방법

개인정보 취급자/홈페이지 이용자가 작성한 게시물에 개인정보가 포함되어 있는 경우, 게시물을 비공개 전환하여 개인정보가 노출되지 않도록 임시조치하고, 해당 페이지를 삭제하거나 개인정보를 123456-1******와 같이 마스킹 처리 한 후 재등록해야 합니다.

[그림 33] 게시글/댓글 내 개인정보 노출 시 조치 절차

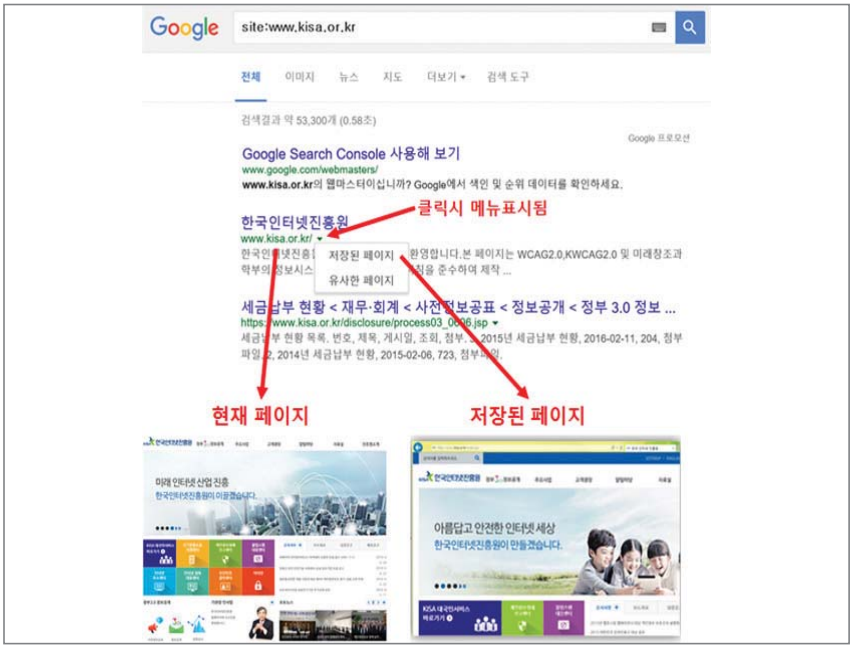
마지막으로, 노출된 페이지의 처리가 끝난 후에는 항상 검색엔진에서 해당 페이지가 수집되었는지 확인하고, 수집된 페이지가 있을 시 삭제요청을 하여야 합니다.

처리절차 (예시)

Step 1. 게시물을 비공개로 전환
Step 2. 게시글 삭제 또는 개인정보를 123456-1******와 같이 마스킹처리하여 재등록
Step 3. (공통사항) 검색엔진에 저장된 페이지 삭제(Ⅲ.4 참조)

4. 검색엔진에 저장된 페이지 삭제 방법 공통사항

개인정보가 노출되었을 경우 노출된 페이지에 있는 개인정보를 삭제하였어도, 검색엔진은 삭제하기 이전의 홈페이지 정보를 저장하고 있으며, 이를 캐시페이지라고 합니다.



[그림 34] 검색엔진에 저장된 페이지 확인 방법

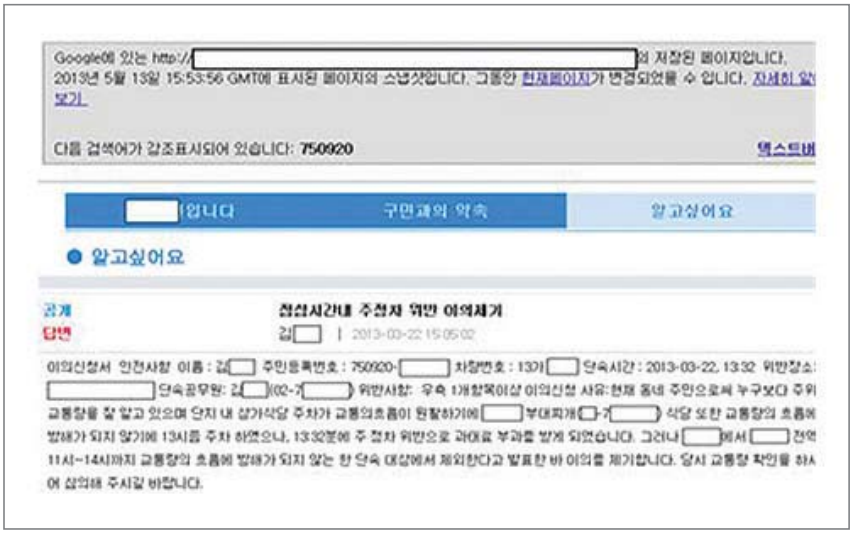
저장된 페이지(캐시페이지)의 갱신(Update)은 별도의 삭제 요청을 하지 않는 경우, 검색엔진 종류에 따라 몇 주에서 수개월이 소요됩니다.

따라서, 개인정보가 노출되었을 경우에는 노출된 홈페이지나 첨부파일에 대한 개선조치 이후에 검색엔진에 수집된 홈페이지를 삭제해 달라는 요청을 하는 것이 좋습니다.(삭제 요청 시 1일~3일 소요)

가. 개인정보가 노출된 페이지 또는 파일 검색

개인정보가 노출된 페이지를 삭제 또는 수정하였을 경우 검색엔진에서 노출된 페이지의 URL 또는 노출된 값을 이용하여 페이지를 검색합니다. (참고3. 구글 웹 마스터 도구 사용법 참조)

검색의 결과에서 [그림 35]와 같이 캐시페이지에 개인정보가 존재할 경우에는 검색엔진에 해당 페이지를 삭제해 달라는 요청을 해야 합니다.



[그림 35] 검색엔진 캐시에 저장된 개인정보 노출내역 확인

나. 개인정보가 있는 검색엔진 캐시페이지 삭제요청

각 검색엔진에는 캐시된 페이지에 대해 삭제를 요청하는 별도의 홈페이지를 제공하고 있습니다.

각 검색엔진별로 삭제 요청을 위한 접속 URL 은 아래 표와 같습니다.

[표 7] 검색엔진별 캐시페이지 삭제요청 주소

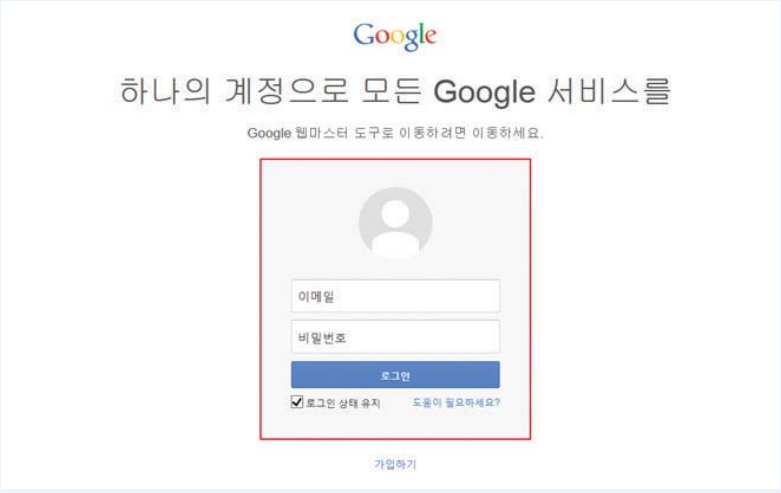
검색엔진	명칭	삭제요청 주소
구글(Google)	오래된 컨텐츠 삭제	https://www.google.com/webmasters/tools/removals
네이버(Naver)	삭제 문의 고객센터	https://help.naver.com/support/home.nhn
다음(Daum)	권리침해 신고센터	https://cs.daum.net/redbell/top.html

그러면 검색엔진별로 삭제를 요청하는 절차를 말씀드리겠습니다.

구글(Google)에 노출된 개인정보 삭제 방법

구글(Google)의 오래된 페이지 삭제(https://www.google.com/webmasters/tools/removals)화면에 접속합니다.

☑ **1단계 계정으로 로그인 합니다.**



[그림 36] 구글 계정 로그인 화면

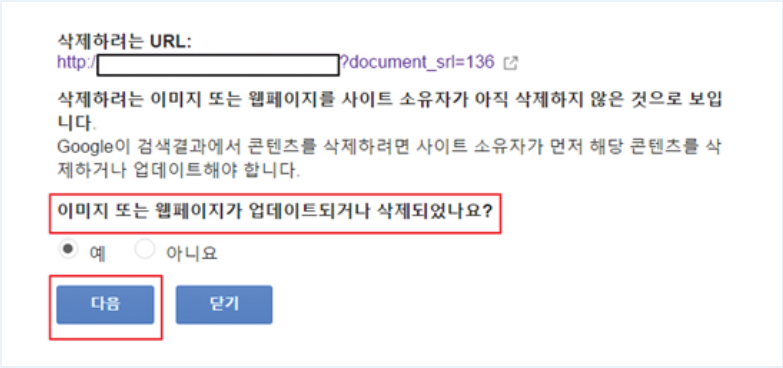
2단계 (삭제할 URL 입력)

[그림 37] 삭제 요청하기 클릭

3단계 (URL 분석 결과, 홈페이지가 삭제된 경우)

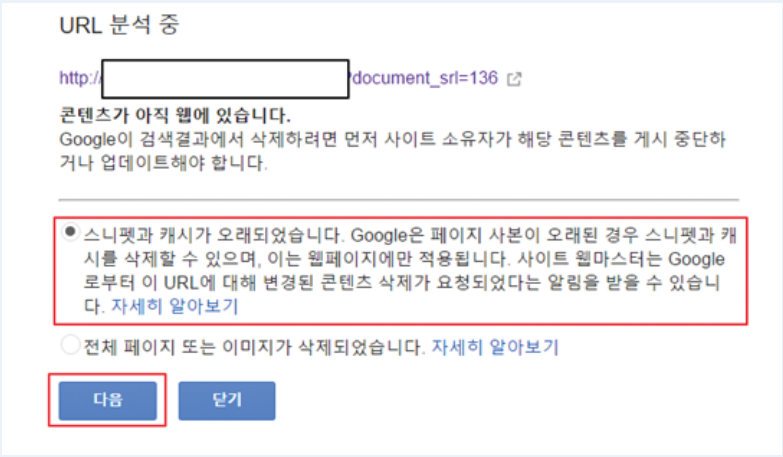
[그림 38] 삭제 요청 클릭

4단계 (URL 분석 결과, 홈페이지에 노출내용은 지웠으나, 페이지가 아직 남아 있는 경우)



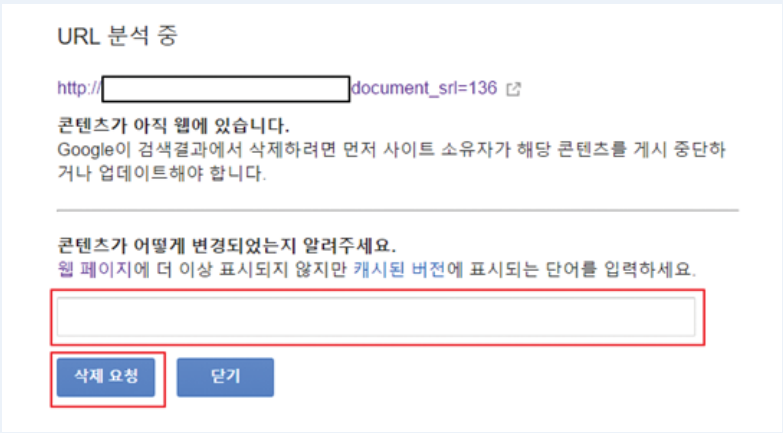
[그림 39] '다음' 으로 진행하기 클릭

5단계 (스니펫 및 캐시 삭제)



[그림 40] '다음' 으로 진행하기 클릭

6단계 (삭제하고자 하는 텍스트 입력)



[그림 41] 삭제 요청 클릭

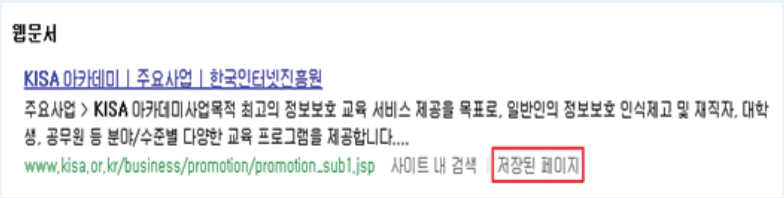
7단계 (삭제 요청 완료, 반영까지 일주일 정도 소요)

[그림 42] 구글(Google) 삭제 확인 및 처리

네이버(Naver)에 노출된 개인정보 삭제 방법

네이버(Naver)의 삭제 문의 고객센터(https://help.naver.com/support/home.nhn)에 접속합니다.

1단계 (삭제할 캐시 페이지 선택)

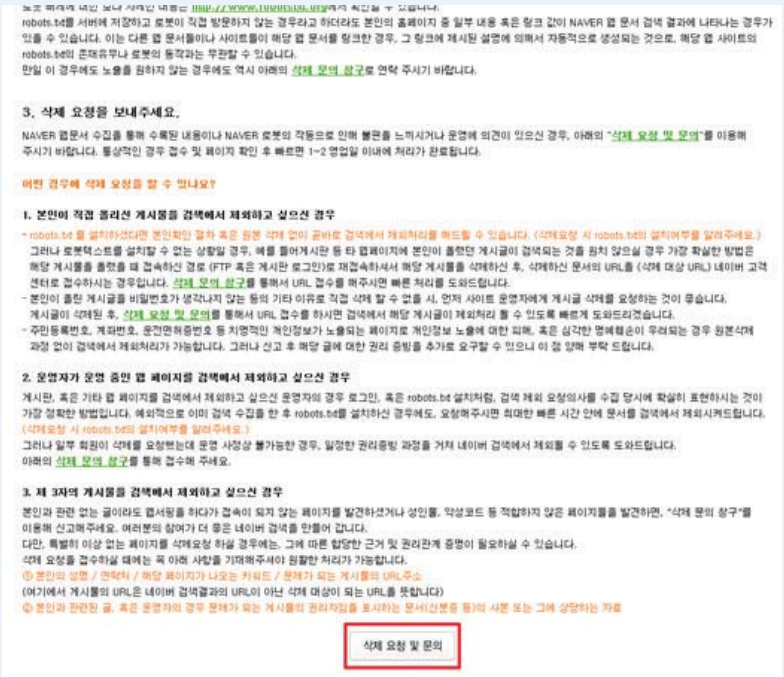


[그림 43] 네이버(Naver) 저장된 페이지 클릭

2단계 (웹문서 삭제 요청 방법 선택)

[그림 44] 네이버(Naver) 웹 문서 삭제 요청 방법 클릭

3단계 (삭제 요청)



[그림 45] 네이버(Naver) 삭제 요청 및 문의 클릭

4단계 (삭제 사유 선택)

[그림 46] 네이버(Naver) 검색 결과 제외 요청하기 화면

5단계 (삭제요청)

[그림 47] 네이버(Naver) 삭제 요청 문의 접수 화면

다음(Daum)에 노출된 개인정보 삭제 방법

다음(Daum)의 권리침해 신고센터(https://cs.daum.net/redbell/top.html) 에 접속합니다.

개인정보가 다음(Daum)에 노출된 경우, 다음(Daum) 고객센터 권리침해 신고를 통해 삭제를 요청할 수 있습니다.

[그림 48] 다음(Daum) 고객센터에서 신고하기 클릭

☑ 1단계 (온라인 접수 방법 선택, 오프라인 신청도 가능함)

[그림 49] 다음(Daum) 개인정보 침해 신고 관련 삭제 접수 방법 선택

2단계 (본인 확인)

[그림 50] 다음(Daum) 실명인증 방법 선택

3단계 (삭제 요청)

[그림 51] 다음(Daum) 개인정보침해 신고 삭제 요청 화면

Ⅳ 개인정보 노출 사전에 예방하세요

key 1. 첨부파일을 업로드하기 전에 개인정보가 있는지 확인하는 것이 좋습니다.

key 2. 관리자페이지는 안전하게 보호하세요.

key 3. 주기적으로 홈페이지의 개인정보 노출여부를 점검하는 것이 좋습니다.

key 4. 게시글에 비공개 설정 기능이 있는 것이 좋습니다.

key 5. 게시글 작성 시 개인정보 노출주의에 대한 안내를 하는 것이 좋습니다.

>> **용어 정의**

Ⅳ 개인정보 노출 사전에 예방하세요

Key 1

첨부파일을 업로드하기 전에 개인정보가 있는지 확인하는 것이 좋습니다.

☞ 업무자료를 공개할 경우, 새로운 파일에 공개할 부분만 복사해서 게시합니다.
☞ 첨부 문서에서 개인정보의 포함여부 확인 후 게시합니다.
  – 숨겨진 Sheet/행/열에 개인정보가 있는지 확인합니다.
  – 문서에 포함된 이미지에 개인정보가 있는지 확인합니다.
  – OLE 객체(그래프 등)는 더블클릭 후 원본자료에 개인정보가 있는지 확인합니다.
☞ 개인정보 검색 제품이 설치된 사용자 PC는 개인정보 포함여부를 점검 후 게시합니다.

Key 2

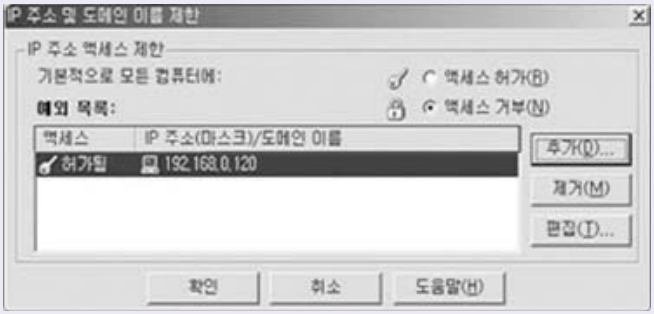
관리자페이지는 안전하게 보호하세요.

☞ 관리자 페이지에 외부접속이 필요할 경우, 전용선이나 가상사설망(VPN)을 이용합니다.
☞ 관리자 페이지는 관리자만 접속할 수 있도록 IP를 제한합니다.
☞ 관리자 페이지는 보안서버(SSL)를 적용하여 통신구간을 암호화합니다.
☞ 관리자 페이지는 인증된 관리자만 접속할 수 있도록 임의 접근을 제한합니다.
☞ 관리자 페이지의 주소에 추측 가능한 단어(admin, manager 등) 사용을 자제합니다.

관리자페이지 접근제한의 설정

1. IIS 웹서버(윈도우즈 서버)의 경우

– '설정 〉 제어판 〉 관리도구 〉 인터넷 서비스 관리자' 선택
– 해당 관리자페이지 폴더에 오른쪽 클릭을 하고 등록정보 〉 디렉터리 보안 〉 IP 주소 및 도메인 이름 제한 〉 편집 버튼을 클릭
– 액세스 거부를 선택하고 추가 버튼을 클릭하여 관리자 호스트IP 또는 서브넷을 등록



2. Tomcat 서버의 경우

– $CATALINA_HOME(톰캣 홈 디렉터리)/conf/server.xml 파일 내용 중 〈Host〉 부분
– 필드 사이에 아래와 같은 설정을 추가한 후 서버를 재시작하면 관리자페이지에 대해 IP기반으로 어용된 IP만 접근이 가능하도록 제어가 가능

Tomcat 서버설정 예

```
〈Host ...〉
〈Context path=" /KISAadm"  docBase=" /tomcat/webapps/ROOT/KISAadm" 〉
〈Valve className=" org.apache.catalina.valves.RemoteHostValve"
allow=" 192.168.1.2" /〉
〈/Context〉
〈/Host〉
```

※ 한국인터넷진흥원 홈페이지(http://www.kisa.or.kr) 〉 자료실 〉 관련법령·기술안내서 〉 기술안내서 가이드 〉 홈페이지 개발보안 안내서(p40), 홈페이지 취약점 진단제거 가이드(p67)

Key 3

주기적으로 홈페이지의 개인정보 노출여부를 점검하는 것이 좋습니다.

☞ 웹사이트 변경(통합, 개선, 복구 등)시 다음 사항을 점검 합니다.
- 웹 취약점 진단 및 시큐어 코딩 준수여부 점검 합니다.
- 회원 식별자를 개인정보로 사용하고 있는지 점검 합니다.
- 암호화 대상인 개인정보의 암호화 여부를 점검 합니다.
- 변경된 웹사이트는 외부에 공개하기 전에 개인정보 포함 여부를 점검 합니다.

☞ 주기적으로 외부 검색엔진에 개인정보가 수집되는지 점검 합니다.
- 검색엔진 고급검색 기능을 이용하여 개인정보를 주기적으로 점검 합니다.
  (검색단어 : “번호” , “주민” , “전화” , “여권” 등 활용)
- 디렉터리 리스팅 여부를 점검 합니다.
  ※ [참고 3] 구글 웹마스터 도구 사용법 참조

Key 4

게시글에 비공개 설정 기능이 있는 것이 좋습니다.

☞ 자주 묻는 질문(Q&A) 게시판과 1:1 상담 게시판을 분리하여 운영합니다.
- Q&A 게시판은 담당자가 관리하고 누구나 읽을 수 있도록 공개로 운영합니다.
- 1:1 상담 게시판은 작성자와 담당자만 읽을 수 있도록 비공개로 운영합니다.

※ 민원, 신청서 업로드 등 개인정보가 포함될 가능성이 많은 게시판은 비공개로 운영합니다.

☞ 개인정보가 포함된 경우, 즉시 삭제할 수 없을 때는 비공개로 전환합니다.

Key 5

게시글 작성 시 개인정보 노출주의에 대한 안내를 하는 것이 좋습니다.

☞ 홈페이지 이용자가 게시판을 이용 시 개인정보 노출예방에 대한 안내를 받을 수 있도록 글 작성 페이지에 안내글이나 팝업창을 제공 합니다.

용어 정의

이 안내서에서 사용하는 용어의 뜻은 다음과 같습니다.

용어	용어 정의
개인정보	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다. (개인정보 보호법 제2조)
개인정보 마스킹	개인정보 보호를 위해 주민등록번호, 의료보험번호, 여권번호, 운전면허번호 같은 개인정보의 일부분을 블라인드 처리하여 표시하는 방법을 말합니다.
개인정보 검색 솔루션	홈페이지 내에 존재하는 개인정보를 검색하여 개인정보의 위치를 확인해주는 솔루션을 말합니다.
개인정보 차단 솔루션	홈페이지 내에 게시글 등록 시 본문 내용 또는 첨부되는 파일 안에 주민등록번호, 휴대폰번호 등 개인정보가 포함되어 있는지 검사 후 차단하는 솔루션을 말합니다.
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말합니다. (개인정보 보호법 제2조)
개인정보취급자	개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자를 뜻합니다. (개인정보 보호법 제28조)
검색엔진 (Search Engine)	인터넷상의 웹 사이트에 있는 각종 정보를 검색해주는 기능을 제공하는 프로그램입니다. 검색 엔진은 크게 웹 사이트를 검색하여 해당 정보를 수집하는 로봇 에이전트와 수집된 자료가 저장되는 데이터베이스, 그 데이터베이스에서 자료를 검색하는 검색 프로그램으로 구성됩니다. 로봇 에이전트가 인터넷을 검색하여 수집한 정보들의 위치를 데이터베이스로 구축해 놓고, 이용자가 검색어를 입력하면 관련된 정보의 위치를 알려 줍니다.
공공기관	국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체와 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관을 말합니다.
디렉터리 (Directory)	디지털 자료 저장장치인 하드디스크에 저장된 파일들을 담고 있는 영역을 말하며, 디렉터리에는 그 속에 저장된 각각의 파일에 대한 이름과 크기, 위치 등이 기록되어 있습니다.
디렉터리 리스팅 취약점 (Directory Listing Vulnerability)	WEB이나 FTP 서비스의 취약한 설정으로 인해 서버의 디렉터리 및 파일에 열람 및 다운로드가 가능하게 되는 취약점입니다. 인터넷 이용자가 모든 디렉터리 및 파일 목록을 볼 수 있어 비공개 자료가 유출될 수 있습니다.

용어	용어 정의
보이스피싱 (Voice Phishing)	전화를 통해 불법적으로 개인 정보(주민등록번호, 신용카드번호, 은행계좌번호 등)를 빼내 범죄에 사용하는 신종 전화 사기 수법입니다. 음성(voice), 개인 정보(personal information) 및 낚시(fishing)를 합성한 신조어입니다. 기존의 피싱은 이메일을 통해 중요 정보를 입력하게 하는 소극적인 방법인 데 반해, 보이스피싱은 범행 대상자에게 전화를 걸어 송금을 요구하거나 개인 정보를 수집하는 적극적인 방법입니다.
세션 (Session)	네트워크 환경에서 사용자간 또는 컴퓨터 간 대화를 위한 논리적 연결을 의미합니다.
소스코드 (Source Code)	컴퓨터 프로그램을 만들기 위해 프로그래밍 언어로 기술한 글을 말합니다.
스팸 (Spam)	수신자의 의사와 관계없이 인터넷상의 다수 수신인에게 전자 우편(e-mail), 문자 메시지 등을 이용하여 무더기로 발송된 광고나 선전물을 의미합니다.
엑셀 (Excel)	미국 마이크로소프트(MS)사에 개발한 PC 용 수치관리 프로그램을 의미합니다. 많은 스프레드시트를 연결, 통합하여 다양한 도형과 차트 등 설명 자료를 작성하는 기능을 제공합니다.
웹 서버 (Web server)	웹 페이지가 들어 있는 파일을 이용자들에게 제공하는 프로그램입니다. 웹 사이트를 통해 서비스를 하려면 웹 서버 프로그램을 설치해야 합니다. 보편적인 웹 서버로는 아파치와 인터넷 인포메이션 서버, 엔터프라이즈 서버 등이 있습니다.
전용선	데이터 통신 등에서 각 장치들을 연결하는 회선으로 그 연결된 장치들만 사용할 수 있는 회선을 뜻합니다.
정규표현식	특정한 규칙을 가진 문자열의 집합을 표현하는 데 사용하는 형식 언어입니다. 정규표현식은 많은 텍스트 편집기와 프로그래밍 언어에서 문자열의 검색과 치환을 위해 사용하고 있습니다.
정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말합니다. (개인정보 보호법 제2조)
개인정보의 처리	개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다. (개인정보 보호법 제2조)
캐시 (Cache)	데이터 접근을 빠르게 할 수 있도록 미래의 요청에 대비해 데이터를 일시 저장해 두는 장소를 말합니다.

용어	용어 정의
크롤러 (수집기)	웹상의 다양한 정보를 자동으로 검색하고 색인하기 위해 검색엔진을 운영하는 사이트에서 사용하는 소프트웨어입니다. 사람들이 일일이 해당 사이트의 정보를 검색하는 것이 아니라 컴퓨터 프로그램의 미리 입력된 방식에 따라 끊임없이 새로운 웹 페이지를 찾아 종합하고, 찾아진 결과를 이용해 또 새로운 정보를 찾아 색인을 추가하는 작업을 반복 수행합니다. 스파이더(spider), 봇(bot), 또는 지능 에이전트라고도 합니다.
팝업창	특정 홈페이지가 어떠한 내용을 표시하기 위해 갑자기 생성되는 새 창을 말합니다.
포워드 (Forward)	클라이언트가 접속한 서버에서 다른 서버로 페이지 변경이 발생하는 경우를 말합니다.
포털사이트 (Portal Site)	인터넷의 출발점과 관문이 되는 사이트를 말하는데, 초기에는 인터넷을 항해하기 위한 출발점으로서의 역할만을 수행하였습니다. 그러나 현재는 특정 주제를 가지고 한 영역에서 전문정보를 제공하는 서비스나 필요한 모든 서비스를 한 사이트를 통해 제공받는 서비스를 의미합니다.
휴면 홈페이지	휴면 홈페이지는 장기간 동안 접속자가 없거나 관리가 이루어지지 않고 방치된 웹 사이트를 말합니다.
OLE (Object Linking and Embedding)	응용 프로그램 간 서로 호환이 되어 다른 응용 S/W에서 작성한 그림이나 표, 차트, 비디오 등과 같은 데이터의 정보를 연결시켜 주는 기능을 뜻합니다.
OWASP (The Open Web Application Security Project)	1984년 4월 안전한 웹 및 어플리케이션을 개발할 수 있도록 지원하기 위해 미국에서 비영리 단체로 출발한 전 세계 기업, 교육기관 및 개인이 만들어가는 오픈 소스 애플리케이션 보안 프로젝트입니다.
OWASP 10대 취약점	웹 애플리케이션 취약점 중에서 빈도가 높고, 보안상 악영향을 줄 수 있는 것들 10가지를 선정한 것입니다. ※ [참고 2] OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점 참조
VPN (Virtual Private Network)	인터넷망을 전용선처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 기술로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용합니다.
URL (Uniform Resource Locator)	흔히 URL을 웹 사이트 주소로 알려져 있지만, 이는 웹 사이트 주소뿐만 아니라 컴퓨터 네트워크 상의 모든 자원을 나타낼 수 있습니다. URL은 주 컴퓨터의 이름과 주소, 파일이 있는 디렉터리 위치, 파일 이름으로 구성됩니다.

홈페이지 개인정보 노출방지 안내서

>>>> 참고 1 홈페이지 개인정보 유출 시 신고절차

>>>> 참고 2 OWASP에서 발표한 10대 웹 애플리케이션 보안 취약점

>>>> 참고 3 구글 웹마스터 도구 사용법

>>>> 참고 4 로봇배제표준

>>>> 참고 5 고유식별정보 정규표현식

참고 1 홈페이지 개인정보 유출 시 신고절차

개인정보 처리자는 정보주체의 개인정보가 유출된 경우에 정보주체에게 지체 없이 통지하고 조치결과를 관계 중앙행정기관(행정자치부장관, 방송통신위원회) 또는 한국인터넷진흥원에 지체 없이 신고하여야 합니다.

다만, 오프라인 사업자의 경우에는 유출된 개인정보가 1만 명 이상인 경우에 행정자치부장관 또는 한국인터넷진흥원에 신고하면 됩니다.

[참고] 개인정보 보호법에서 '개인정보 유출 통지 및 신고' 처리에 대한 관련 법령은 다음과 같습니다.

관련 법령

[개인정보 보호법] 제34조 제3항(개인정보 유출 통지 등)

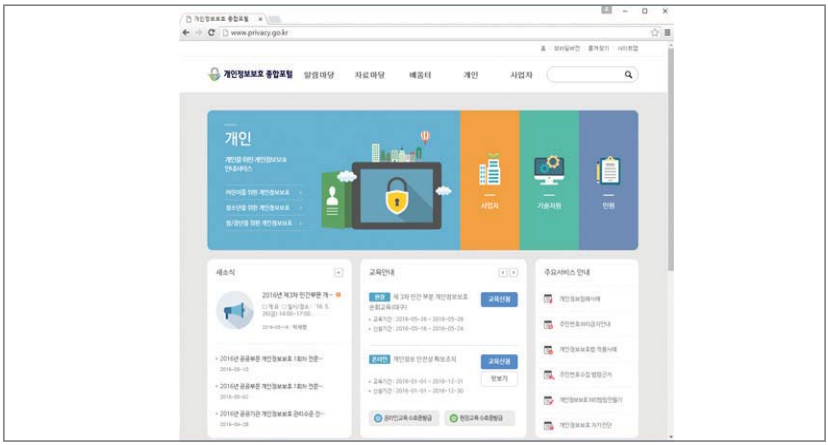
③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

[개인정보 보호법 시행령] 제39조제1항(개인정보 유출 신고의 범위 및 기관)

① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 1만 명 이상의 정보주체에 관한 개인정보를 말한다.

개인정보보호 종합포털을 통해 한국인터넷진흥원으로 온라인 신고하는 절차는 다음과 같습니다.

☑ 1단계 (개인정보보호 종합포털(www.privacy.go.kr)에 접속)

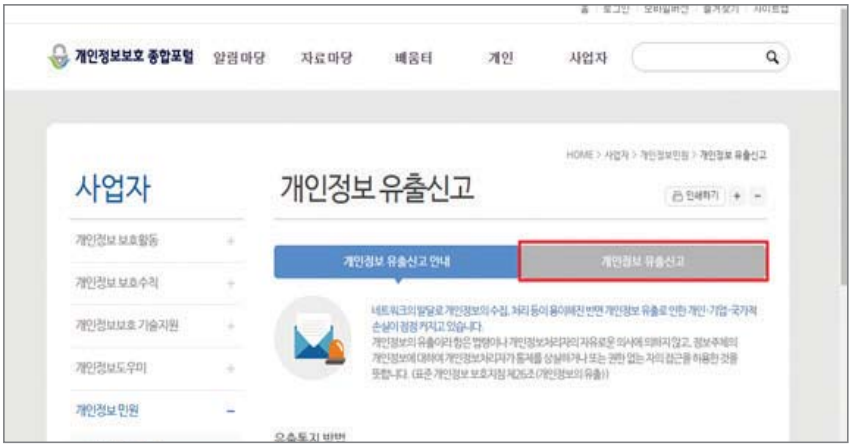


[그림 52] 개인정보보호 종합포털 화면

☑ 2단계 (사업자 메뉴 > 개인정보 민원 클릭)

[그림 53] 개인정보 민원 메뉴선택

3단계 (화면 우측 상단의 "개인정보 유출신고" 선택)



[그림 54] 개인정보 유출신고 선택

4단계 (웹 페이지 메시지 확인 후 "확인" 선택)

[그림 55] 개인정보 유출신고 메시지 확인

5단계 (개인정보 유출신고 작성)

[그림 56] 개인정보 유출신고 화면

[참고] 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 '개인정보 유출 통지 및 신고' 처리에 대한 관련 법령은 다음과 같습니다.

☑ 관련 법령

[정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제27조의3 제1항(개인정보 누출등의 통지·신고)

① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등" 이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 〈개정 2014.5.28.〉

[정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제27조의3 제1항(개인정보 유출등의 통지·신고)

① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등" 이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 〈개정 2014.5.28., 2016.3.22.〉[본조신설 2012.2.17.] [제목개정 2016.3.22.] [시행일 : 2016.9.23.] 제27조의3

※ 2016년 9월 23일 이후로 제27조의3 제1항(개인정보 누출등의 통지·신고)가 제27조의3 제1항(개인정보 유출등의 통지·신고)로 변경됩니다.

[정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령] 제39조제1항(개인정보 누출 등의 통지·신고)

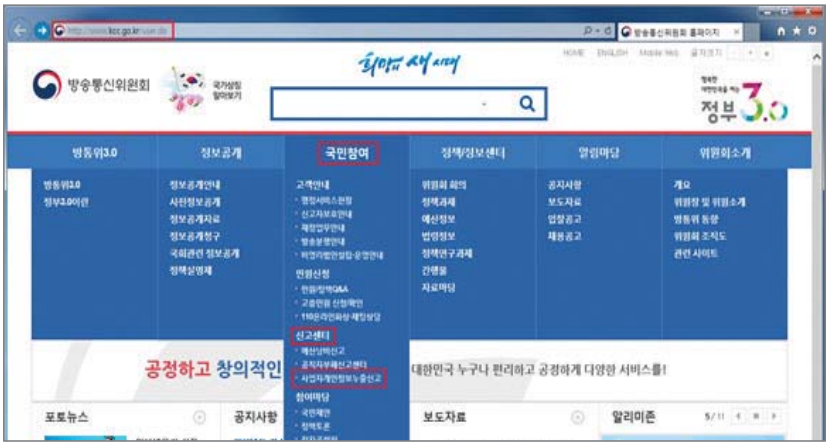
① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등" 이라 한다)의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.

개인정보보호 포털을 통해 방송통신위원회로 유출신고 하는 방법은 서면 신고와 온라인 신고로 구분되어 있습니다.

☑ 1단계 (방송통신위원회(www.kcc.go.kr)에 접속)

[그림 57] 방송통신위원회 홈페이지 화면

2단계 (국민참여 메뉴 > 신고센터 클릭 > 사업자 개인정보 누출신고 클릭)



[그림 58] 사업자 개인정보 누출신고 메뉴선택

3단계 (개인정보보호 포털(www.i-privacy.kr)로 이동)

[그림 59] 개인정보보호 포털 화면

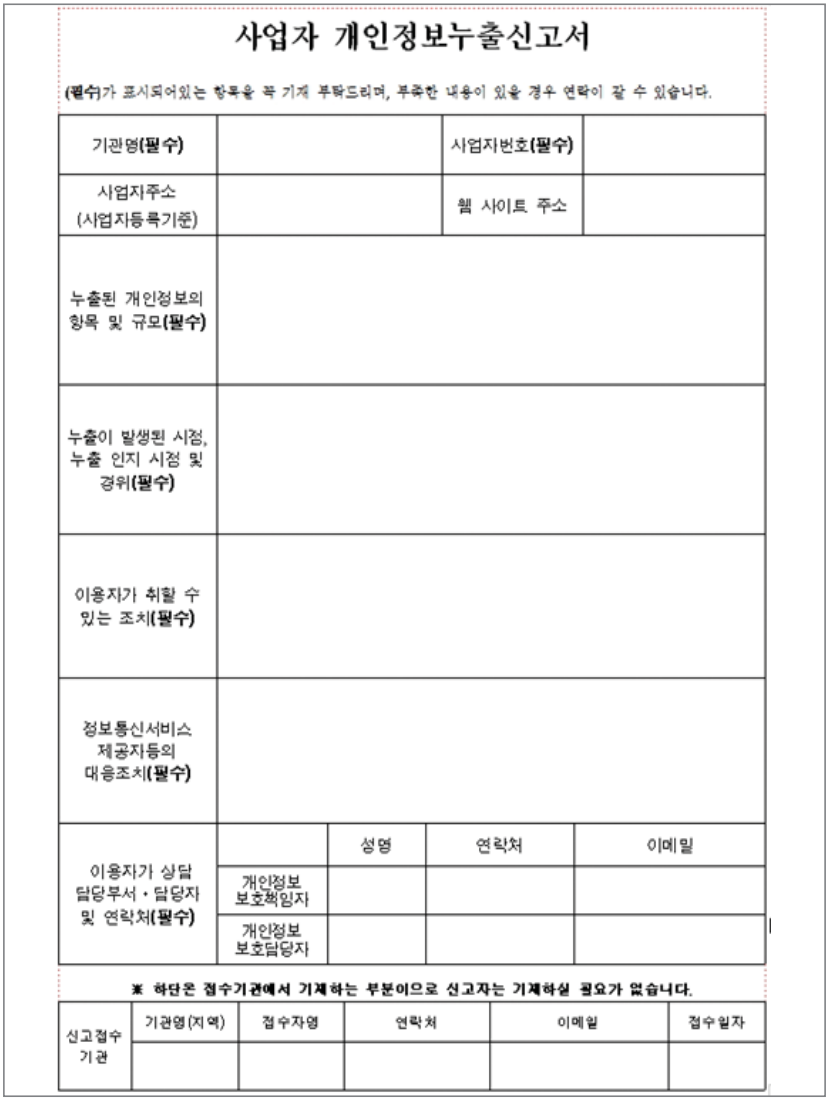
4단계 (개인정보 신고 메뉴 > 개인정보 누출신고 클릭)

[그림 60] 개인정보 누출신고 메뉴선택

5단계 [서면신고]의 경우 ('개인정보 누출신고 다운로드'를 클릭하여 양식 다운로드)

[그림 61] 개인정보 누출신고서 다운로드 선택

6단계 [서면신고]의 경우 (다운로드 받은 '사업자_개인정보 누출신고서'에 신고내용을 작성)



사업자 개인정보누출신고서

(필수)가 표시되어있는 항목을 꼭 기재 부탁드리며, 부족한 내용이 있을 경우 연락이 갈 수 있습니다.

기관명(필수)		사업자번호(필수)	
사업자주소 (사업자등록기준)		웹 사이트 주소	
누출된 개인정보의 항목 및 규모(필수)			
누출이 발생된 시점, 누출 인지 시점 및 경위(필수)			
이용자가 취할 수 있는 조치(필수)			
정보통신서비스 제공자등의 대응조치(필수)			

이용자가 상담 담당부서·담당자 및 연락처(필수)		성명	연락처	이메일
	개인정보 보호책임자			
	개인정보 보호담당자			

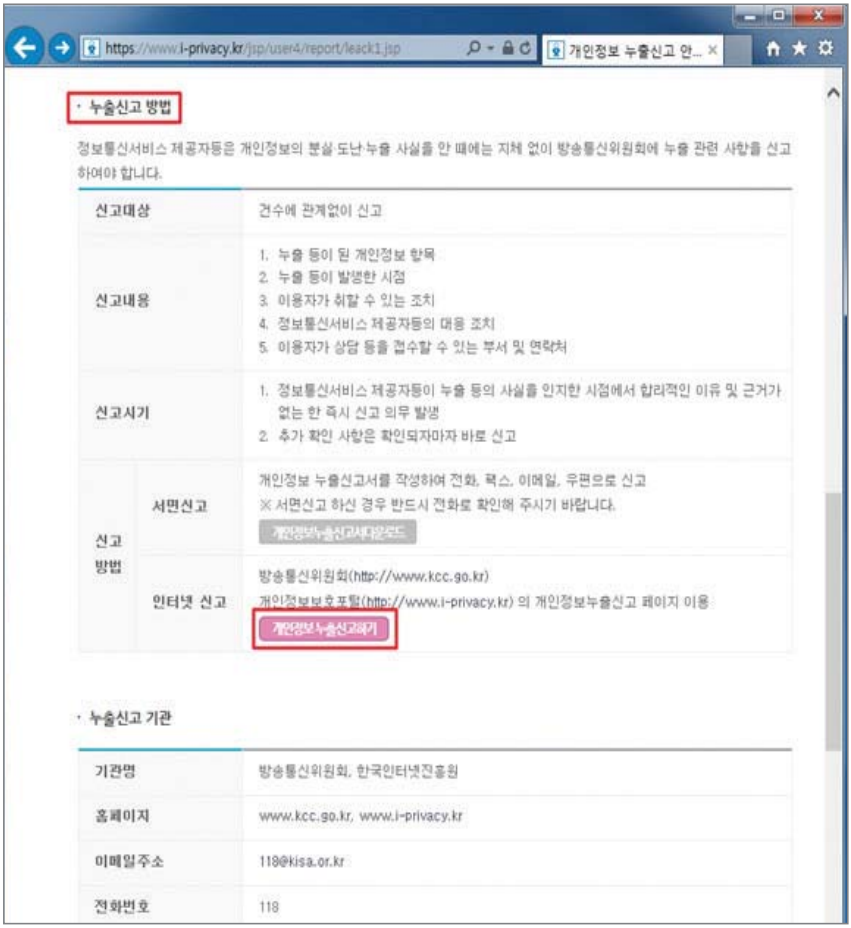
※ 하단은 접수기관에서 기재하는 부분이므로 신고자는 기재하실 필요가 없습니다.

신고접수 기관	기관명(지역)	접수자명	연락처	이메일	접수일자

[그림 62] 사업자 개인정보 누출신고서 양식

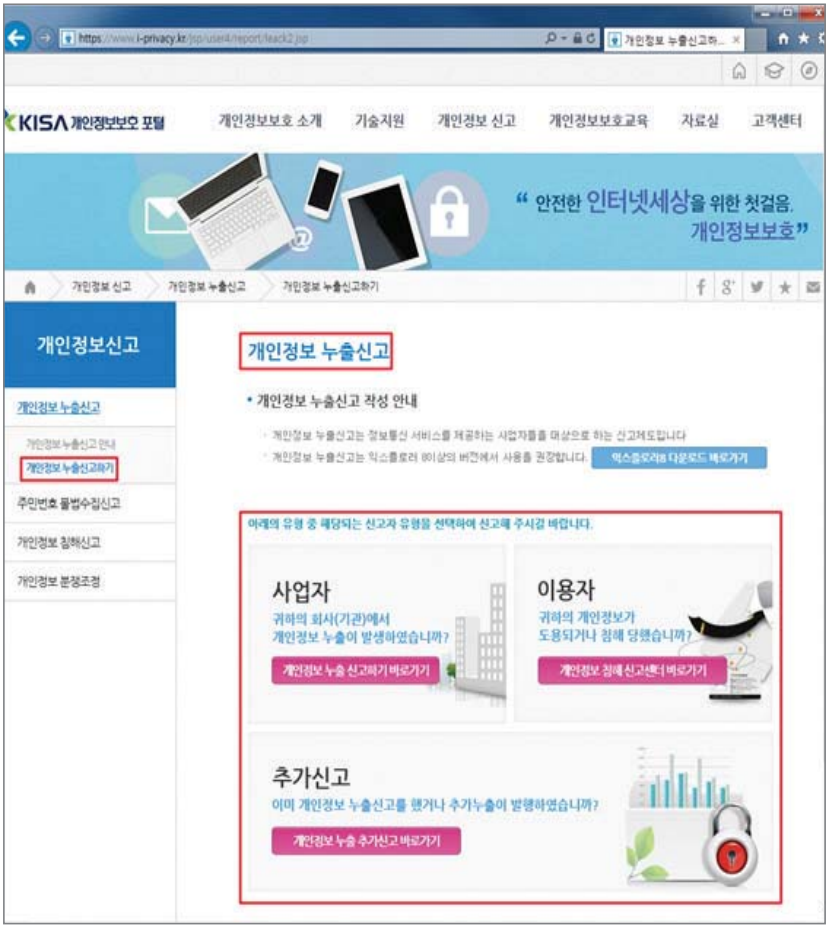
※ 서면신고의 경우 누출신고서를 작성하여 전화, 팩스, 이메일, 우편으로 신고하시면 됩니다.
연락처는 [그림 61]의 누출신고 기관 연락처를 참고하시면 됩니다.

☑ 5단계 [인터넷 신고]의 경우 ('개인정보 누출신고하기'를 클릭)



[그림 63] 개인정보 누출신고하기 클릭

6단계 [인터넷 신고]의 경우 (3가지 유형 중 해당되는 신고자 유형을 클릭 후 신고)



[그림 64] 신고자 유형 선택

참고 2 OWASP[1] 에서 발표한 10대 웹 애플리케이션 보안 취약점

[표 8] 2013년 OWASP 10대 보안 취약점

항목	내용
A1. 인젝션 (Injection)	이용자가 입력한 데이터가 명령어나 질의문의 일부분으로 웹 서버의 데이터베이스나 백엔드 시스템의 인터프리터에 연결되어 명령어 실행 및 데이터 변경이 실행되는 취약점
A2. 취약한 인증 및 세션관리 (Broken Authentication and Session Management)	계정에 대한 증명과 세션토큰이 적절히 보호되지 못함으로 인해 패스워드나 키, 세션쿠키, 다른 토큰 등을 악용하여 인증 메커니즘을 무력화 시키거나 다른 이용자의 아이디를 추측할 수 있는 취약점
A3. 크로스사이트 스크립트(XSS) (Cross-Site Scription)	악의적인 공격자가 타인의 브라우저 내에서 스크립트를 실행하도록 허용함으로써 타인의 세션을 가로채거나 웹 사이트를 손상하거나 웜을 삽입하는 등을 가능하게 하는 취약점
A4. 불안전한 직접객체 참조 (Insecure Direct Object References)	파일, 디렉터리, 데이터베이스 기록, 키 등의 내부 구현 객체에 대한 참조 정보를 URL 또는 폼 파라미터로 노출시켜서 악의적인 공격자가 이를 조작하여 인증절차 없이 다른 객체에 접속할 수 있도록 하는 취약점
A5. 보안상 잘못된 구성 (Security Misconfiguration)	어플리케이션, 프레임워크, 어플리케이션 서버, 웹 서버, 데이터베이스 서버와 플랫폼에 대한 적절한 보안 구성에 대한 정의 및 적용 여부, 어플리케이션 코드 라이브러리를 포함한 소프트웨어의 최신 업데이트 유지
A6. 민감한 데이터 노출 (Sensitive Data Exposure)	카드번호 같은 민감한 데이터를 암호화하지 않거나 데이터 전송 시 암호화 등을 거치지 않아 악의적인 공격자에 의해 민감 데이터가 노출되는 취약점
A7. 기능접근제어누락 (Missing Function Level Access Control)	어플리케이션은 각 기능에 대한 접근 시 동일한 접근제어검사 수행이 요구됨. 접근제어검사가 적절하지 않을 경우 악의적인 공격자는 비인가된 기능에 접근하기 위해 정상적인 요청을 변조할 가능성이 있음
A8. 크로스사이트 변조요청(CSRF) (Cross-Site Request Forgery)	로그온을 한 이용자의 브라우저가 사전에 승인된 요청을 웹 서버에 보내도록 함으로써 악의적인 공격자가 의도하는 공격을 수행하도록 하는 취약점
A9. 취약점이 있는 컴포넌트 사용 (Using Known Vulnerable Components)	슈퍼유저권한으로 운영되는 취약한 컴포넌트(라이브러리, 프레임워크 및 기타 소프트웨어 모듈)로 인해 데이터 유실 및 서버 권한 획득과 같은 취약성 존재
A10. 검증되지 않은 리다이렉트와 포워드(Unvalidated Redirects and Forwards)	웹 어플리케이션은 목적페이지를 결정하기 위해 신뢰되지 않은 데이터를 사용하기 때문에 적절한 확인이 없다면, 공격자는 피싱사이트나 악의적인 사이트로 리다이렉트 유도 및 권한없는 페이지에 포워드를 시도함

1) OWASP(Open Web Application Security Project)

1984년 4월 안전한 웹 및 응용을 개발할 수 있도록 지원하기 위해 미국에서 비영리 단체로 출발한 전 세계 기업, 교육기관 및 개인이 만들어가는 오픈 소스 애플리케이션 보안 프로젝트

참고 3 구글 웹마스터 도구 사용법

1. 서치 콘솔(Search Console) 도움말

구글(Google)의 저장된 페이지에서 개인정보가 노출될 경우, 구글에서 제공하고 있는 웹마스터 도구를 이용하여 검색엔진의 "저장된 페이지" (캐시)를 삭제요청 할 수 있습니다. 웹마스터 도구 삭제 요청 절차를 자세히 살펴보도록 하겠습니다.

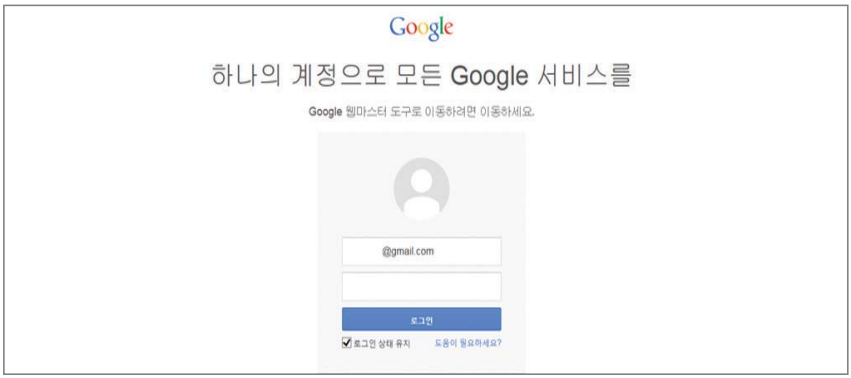
구글(Google) 웹마스터 도구란 이용자 페이지의 게재빈도와 관련된 자세한 보고서를 제공해주고 홈페이지에 대한 정보를 확인할 수 있게 해주는 도구입니다.

[그림 65] 구글 웹마스터 도구 도움말 접속 화면

참조 : 구글 웹마스터 도구 도움말 :
https://support.google.com/webmasters/?hl=ko#topic=3309469

가. 구글 웹마스터 도구에서 홈페이지의 소유권 확인 방법

1단계 (로그인)



[그림 66] 구글 웹마스터 도구 로그인

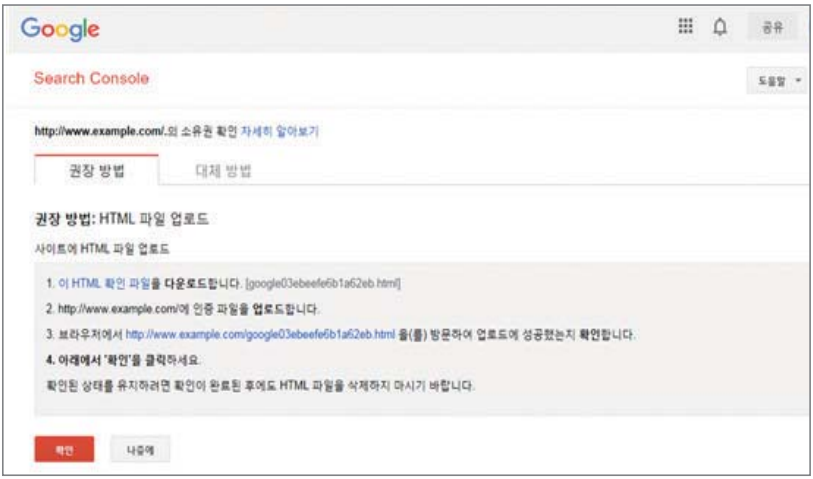
2단계 (사이트 추가)

[그림 67] 사이트 추가 클릭

3단계 (사이트 URL 추가)

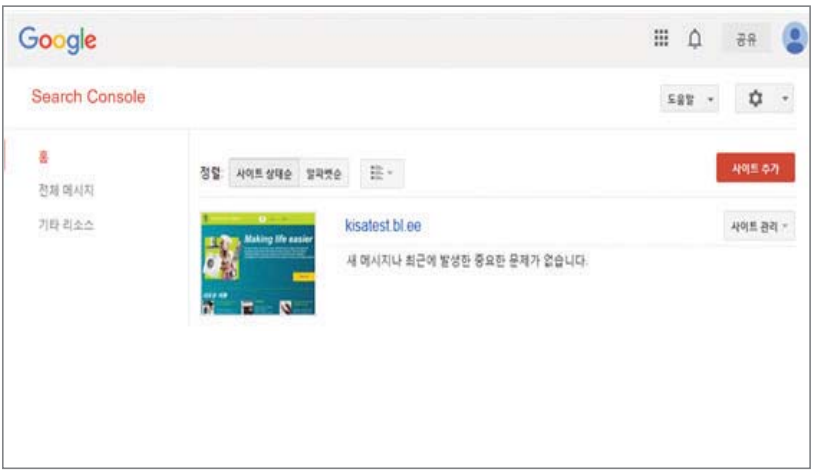
[그림 68] 사이트 URL 입력

4단계 (사이트 소유권 인증)



[그림 69] HTML 파일 업로드

5단계 (사이트 추가 완료)



[그림 70] 사이트 등록 화면

구글 웹마스터 도구에 사이트 등록이 완료되었습니다. 이제 구글 검색엔진에서 검색된 결과를 삭제할 수 있는 방법을 알아보도록 하겠습니다.

사이트에 노출된 개인정보를 삭제하려면 홈페이지에 노출된 개인정보를 삭제한 후 웹마스터 도구를 이용해 캐시에 노출된 페이지를 삭제요청 해야 합니다.

[표 9] 웹마스터 도구를 이용한 삭제방법들의 차이점

삭제방법	차이점	비고
Fetch As Google	검색엔진에 홈페이지 재 수집 요청 기능	사이트소유권확인 필요
	(예시) 홈페이지의 개인정보를 삭제 후 홈페이지 정보를 재수집하도록 요청할 경우 (예시) 다수 페이지에 개인정보가 노출된 경우 (예시) 내부 업무용 게시판, FTP 등에서 개인정보가 노출된 경우	
URL 삭제	긴급하게 사이트를 구글 검색결과에서 삭제하는 기능 (주의) 글 검색결과에서 일시적으로 제외하는 방법이므로 홈페이지조치 미흡 시 재 노출 될 가능성이 있음	
	(예시) 다수 페이지에 개인정보가 노출된 경우	
오래된 콘텐츠 삭제	오래된 캐시 정보 삭제 기능 (참고) 홈페이지가 삭제된 경우, 관리자 아니더라도 삭제 요청 가능	사이트 소유권 확인 필요 없음
	(예시) 홈페이지에서는 삭제되었지만, 캐시에 개인정보가 노출된 경우	

나. 웹마스터 도구 이용 시 주의 사항

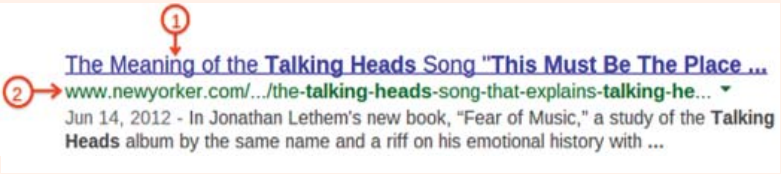
구글 웹마스터 도구를 이용하여 삭제요청을 할 경우, URL을 정확히 입력해야 합니다. URL은 대문자와 소문자를 구분해야 하며, 검색결과에 표시되는 정확한 URL을 입력해야 합니다. 정확한 URL을 확인하는 방법에 대해 알아보도록 하겠습니다.

페이지 URL 찾기

URL 삭제 또는 순위 강등을 요청할 때에는 검색결과에 표시되는 정확한 URL을 입력해야 합니다. URL의 작은 차이(예: www.example.com/dragon과 www.example.com/Dragon)가 중요하지 않게 보일 수 있지만, 예로든 두 URL은 실제로 다른 URL이며 일부 서버에서는 다른 콘텐츠로 연결될 수 있습니다. 검색결과에 표시되는 정확한 URL을 입력해야만 Google에서 원하는 콘텐츠를 삭제하거나 콘텐츠의 순위를 낮출 수 있습니다. 다음은 정확한 URL을 찾기 위한 몇 가지 도움말입니다.

줄임표

검색결과 페이지의 녹색 URL에 줄임표(...)가 포함되어 있으면 대개 화면 표시를 위해 URL을 짧게 표시한 것입니다.



줄임표가 있는 URL은 복사하여 붙여 넣지 마십시요. 대신 검색결과의 제목(위의 이미지에서 1로 표시)을 클릭합니다. 페이지가 열리면 브라우저의 주소 표시줄에서 URL을 복사합니다.

URL을 찾는 또 다른 방법은 검색결과의 링크를 마우스 오른쪽 버튼으로 클릭한 다음 URL을 복사하는 것입니다. 복사한 URL을 URL 삭제 도구 또는 사이트링크 순위 강등 도구에 붙여넣으면 www.google.com으로 시작하는 매우 긴 URL이 표시됩니다. Google에서 올바른 URL을 식별할 수 있으므로 URL이 길어도 걱정하지 마십시요.

대문자 표시

URL 삭제 도구 및 사이트링크 순위 강등 도구는 대소문자를 구분합니다. 즉, www.example.com/nunchuckskills를 입력할 경우 www.example.com/NunchuckSkills는 삭제되거나 순위가 낮아지지 않으며 그 반대의 경우도 마찬가지입니다. 따라서 Google 검색결과에 나타나는 URL과 동일한 대소문자 조합의 URL을 입력해야 합니다. 다시 한 번 강조하지만, 페이지를 열고 주소 표시줄에서 URL을 복사하는 것이 정확한 URL을 얻는 가장 확실한 방법입니다.

이미지

이미지 삭제 요청을 제출하려는 경우 올바른 URL을 찾는 방법은 다음과 같습니다.
1. 이미지 검색결과에 있는 이미지를 클릭합니다.
2. 원본 이미지 보기 또는 전체 크기를 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.
3. URL 삭제 도구에서 사용할 수 있도록 URL을 파일 또는 문서에 붙여넣습니다.

여러 URL

동일한 콘텐츠가 여러 URL에 나오는 것은 일반적이며 포럼 또는 대화목록 기반 홈페이지에서는 이런 경우가 더욱 많습니다. 예를 들면 다음과 같습니다.

http://www.example.com/forum/thread/123
http://www.example.com/forum/post/456
http://www.example.com/forum/thread/123?post=456
http://www.example.com/forum/thread/123?post=456&sessionid=12837460

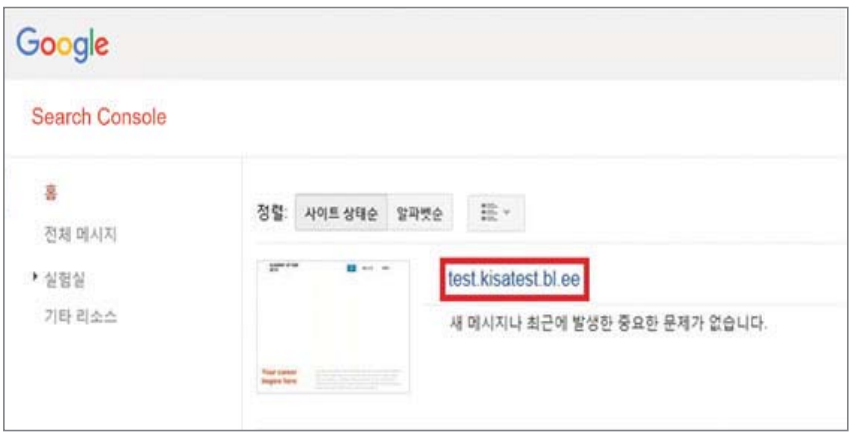
URL 하나의 삭제 또는 순위 강등 요청을 완료한 경우에도 삭제하려는 콘텐츠가 다른 URL로 Google 검색결과에 나타날 수 있습니다. 이 경우에는 이 콘텐츠를 표시하는 각 URL의 삭제 요청을 추가로 제출하면 됩니다.

삭제 요청의 상태가 '삭제됨'으로 표시되지만 검색결과에 삭제 요청한 콘텐츠가 계속 표시되는 경우 검색결과에 나타나는 URL이 삭제를 위해 제출한 URL과 대소문자를 포함하여 정확하게 동일한지 확인해 보세요. 동일하지 않은 경우에는 현재 검색결과에 나타나는 URL의 삭제를 추가로 요청해야 합니다.

[출처] 웹마스터 도구 사용 도움말(https://support.google.com/webmasters/answer/63758?hl=ko)

다. Fetch As Google 이용 방법(사이트 관리자일 경우에만 유효)

1단계 (사이트 선택)



[그림 71] 추가된 도메인 클릭

2단계 (사이트 크롤링 요청)

[그림 72] 'Fetch As Google' 클릭

3단계 (사이트 주소 입력)

[그림 73] 사이트 주소 입력 후 '가져오기' 클릭

4단계 (사이트 재수집 요청)

[그림 74] '색인에 제출' 클릭

5단계 (재수집 범위 선택)

[그림 75] '이 URL 및 직접 연결되는 링크 크롤링' 을 선택 후 확인 클릭

6단계 (사이트 재수집 요청 후 반영까지 일주일 정도 소요)

[그림 76] 삭제 신청 및 확인

라. URL 삭제 이용 방법(사이트 관리자일 경우에만 유효)

구글 검색 결과에서 'URL 제거' 기능은 특정 사이트나 URL을 긴급 삭제하는 기능으로 홈페이지가 삭제되지 않더라도 구글 검색결과에서 임시 삭제됩니다. (임시적인 조치로 검색결과에서는 일정기간 동안만 보이지 않음)

(주의) 삭제 조치가 미흡할 경우 노출될 가능성이 있으므로 홈페이지의 노출된 개인정보 삭제 후 'URL 제거' 기능을 이용해야 합니다.

☑ 1단계 (사이트 선택)

[그림 77] 삭제를 원하는 사이트 선택 클릭

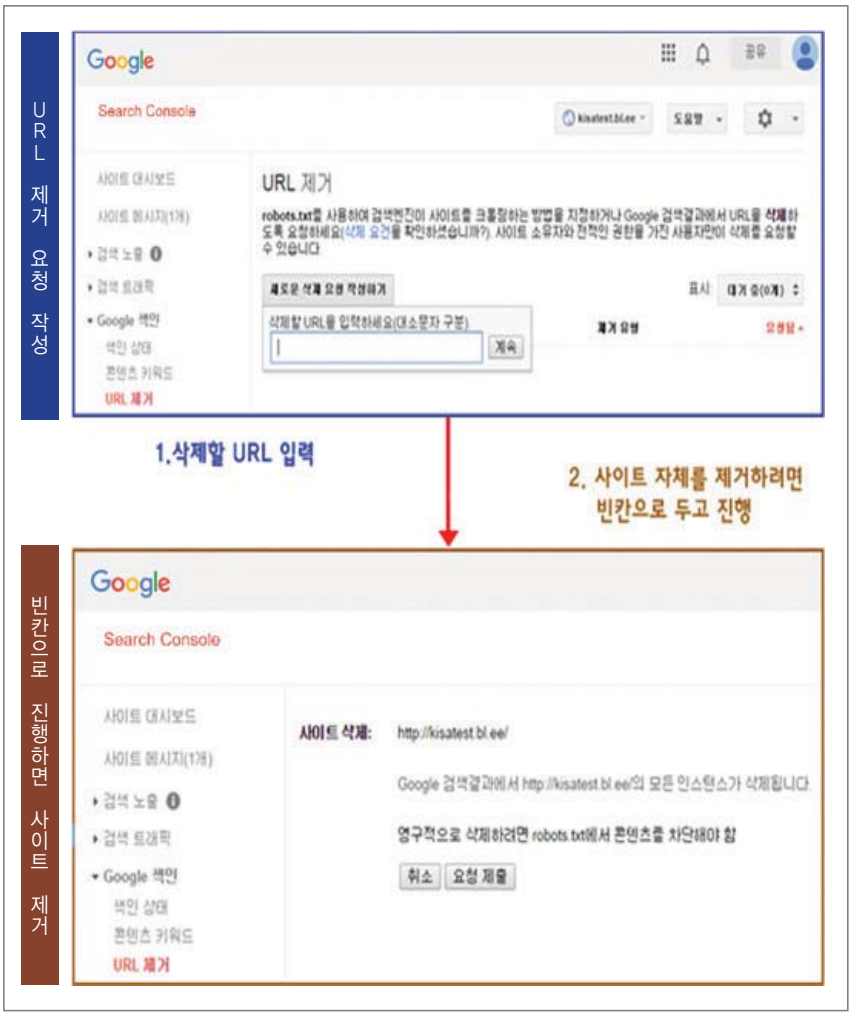
☑ 2단계 (URL 제거 도구 선택)

[그림 78] 'URL 제거' 선택 클릭

☑ 3단계 (삭제 요청)

[그림 79] '새로운 삭제 요청 작성하기' 클릭

4단계 (삭제할 URL 입력, 사이트 자체를 제거하려면 빈칸으로 두고 진행)



[그림 80] 삭제할 URL 입력 후 요청 제출 클릭

5단계 (삭제 사유 선택 후 반영까지 일주일 정도 소요)

[그림 81] 캐시 URL 삭제 이유 선택

[표 10] 캐시 URL을 삭제하고자 하는 이유에 대한 설명

항목	설명
검색결과 및 캐시에서 페이지 삭제	내 사이트 URL에 대한 검색결과 및 캐시페이지를 전부 삭제할 때 신청합니다.
캐시에서만페이지 삭제	사이트에서 페이지를 업데이트하면, 다음에 크롤링 할 때 Google은 캐시된 버전을 비롯하여 색인을 업데이트합니다. 업데이트가 완료될 때까지는 원본 콘텐츠가 캐시에 포함되어 검색결과에 해당 콘텐츠가 표시될 수 있습니다. 오래된 콘텐츠의 삭제를 요청할 수 있으며 이 경우 페이지 미리보기도 삭제됩니다.
디렉터리 삭제	디렉터리나 사이트를 영구적으로 삭제하려면 'robots.txt' 를 사용하여 크롤러가 디렉터리에 액세스하지 못하게 차단하고, 사이트를 삭제하는 경우에는 전체 사이트에 대한 액세스를 차단해야 합니다. 이 작업은 디렉터리 삭제를 요청하기 전이나 요청한 후 곧바로 수행하는 것이 좋습니다. 그렇지 않을 경우, 콘텐츠가 나중에 검색결과에 다시 표시될 수 있습니다.

참고사항

[구글 웹마스터 도구]를 통해 구글 검색결과나 캐시 페이지 삭제요청은 가능하나, 요청을 한다고 해서 반드시 삭제되는 것은 아니며, 구글의 판단에 따라 요청이 거부될 수도 있습니다.

구글의 개인정보 보호정책은 주민등록번호와 같은 국가 발급 번호에 대한 개인정보가 노출 되었을 경우만 삭제 혹은 마스킹(* 처리)이 가능하며, 주민등록번호 이외의 정보에 대해서는 삭제가 되지 않을 수 있습니다.

※ 참조 : 구글 웹마스터도구 FAQ(http://support.google.com/webmasters/answer/1050724?hl=ko)

참고 4 로봇배제표준

가. 개요

로봇배제표준이란 검색로봇의 접근범위를 제한하는 규약으로, 웹 서버에 설정파일(robots.txt)을 만들어 사용합니다.

검색로봇이란 검색엔진이 홈페이지 정보를 수집하기 위해 인터넷을 돌아다니는 소프트웨어를 말합니다.

나. 로봇배제표준에 대한 이해

1) 로봇배제표준은 단순 규약입니다.
로봇배제표준은 국제 표준이 아닌 규약이므로 검색로봇이 반드시 준수하지 않을 수 있습니다.

2) 로봇배제표준은 이용자의 접근과 무관합니다.
로봇배제표준은 검색로봇의 접근범위를 제한하므로, 홈페이지를 이용하는 사람에 대한 접근을 제한하지 않습니다.

3) 로봇배제표준 설정은 누구나 볼 수 있습니다.
robots.txt 파일은 누구나 읽을 수 있으므로 공개된 페이지에 적용하여야 하며, 민감정보(디렉터리, 관리자페이지 정보 등)가 포함되지 않도록 관리자의 주의가 필요합니다.

※ 공개된 페이지 : 글쓰기가 가능하지만 로그인을 하지 않는 게시판 등

4) 로봇배제표준은 개인정보 노출 예방을 위한 임시도구입니다.
보다 안전하게 개인정보 노출을 예방하기 위해서는 기관 담당자가 홈페이지에 개인정보가 게시되지 않도록 주기적인 취약점검, 게시판 비밀번호 설정 및 개인정보 검색/유출차단 시스템 도입 등의 조치를 해야만 합니다.

개인정보 노출 예방을 위해 개인정보 검색/유출차단 솔루션의 도입을 권고하며, 로봇배제표준은 솔루션 도입이 어려운 기관에서 공개된 개인정보가 외부 검색엔진에 검색되는 것을 방지하기 위한 임시도구로 활용하도록 해야 합니다.

다. 로봇배제표준 적용 시 유의점

로봇배제표준은 적용범위에 따라 검색엔진에서 홈페이지 정보가 검색되지 않을 수 있으므로 주의해야 하며, 홈페이지의 용도 및 개인정보 노출방지/차단 솔루션 운영여부 등을 고려하여 기관담당자의 판단에 따라 사용여부를 결정해야 합니다.

라. 로봇배제표준 설정방법

robots.txt 파일의 내용은 크게 2가지로 나뉘는데, 로봇의 이름을 적는 부분(User-agent)과 방문의 허용 여부를 적는 디렉터리 부분(Allow 및 Disallow)으로 구분됩니다.

로봇배제표준 문법을 참고하여 robots.txt 작성한 후 웹 서버의 각 도메인별 최상위 주소에 저장하면 됩니다.

예시) http://www.example.or.kr/robots.txt
※ robots.txt를 다른 디렉터리에 놓는 경우 효력이 없으므로 주의해야 합니다.

1) robots.txt 문법 설명

· (전면허용) 모든 로봇의 접근을 "전면허용" 하는 경우
  User-agent: *
  Allow: /

· (전면차단) 모든 로봇의 접근을 "전면차단" 하는 경우
  User-agent: *
  Disallow: /

· (부분차단) 모든 로봇의 특정 디렉터리 및 파일 접근을 "부분차단" 하는 경우
  User-agent: *
  Disallow: /directory_or_url

· (특정파일) 모든 로봇이 xls 파일에 접근을 차단하는 경우
  User-agent: *
  Disallow: /*.xls

· (특정파일) 특정 로봇의 접근만 "전면허용" 하는 경우 User-agent: 검색로봇명
  Allow:User-agent: *
  Disallow: /

[표 11] robots.txt 작성 시 유의사항

유의사항	잘못된 예시	잘된 예시
대소문자 구분	User-Agent: * disallow: /directory_or_url ※ User-agent의 A가 대문자 ※ Disallow의 d가 소문자	User-agent: *Disallow: /directory_or_url
띄어쓰기	User-agent : * Disallow:/directory_or_url ※ User-agent와 콜론(:)이 떨어짐 ※ Disallow 이후 콜론(:)과 슬래시(/)가 붙음	User-agent: *Disallow: /directory_or_url
줄바꾸기	User-agent: 검색로봇명1 Disallow: /directory_or_url User-agent: 검색로봇명2 Disallow: /directory_or_url ※ 다중 검색로봇을 지정 시, 한 줄을 띄우지 않음	User-agent: 검색로봇명1 Disallow: /directory_or_url User-agent: 검색로봇명2 Disallow: /directory_or_url
설정 파일이름	robot.txt ※ 설정파일 이름은 “robots.txt” 로 해야함	robots.txt
설정파일 적용 위치	examle.or.kr/sub_directory/robots.txt ※ 파일 위치는 홈페이지의 최상위 디렉터리(/)이어야 함	example.or.kr/robots.txt
적용대상	www.example.or.kr ※ 기관 홈페이지가 복수 개인 경우 (각각 도메인이 다른 경우) 모두 개별적으로 적용해야 함	http://www.example.or.kr http://example.or.kr https://www.example.or.kr http://edu.example.or.kr http://media.example.or.kr

[표 12] 검색엔진별 검색로봇 리스트

검색엔진	검색로봇
다음	Daumoa
구글	Googlebot
야후	Yahoo! Slurp
네이버	Naverbot
Bing	Bingbot
Microsoft	Msnbot
네이트	Natebot

참고 5 고유식별정보 정규표현식

개인정보를 검사하는 정규표현식(패턴)

▶ 주민등록번호
([01][0-9]{5}[[:space:],~-]+[1-4][0-9]{6}|[2-9][0-9]{5}[[:space:],~-]+[1-2][0-9]{6})

▶ 여권번호
[a-zA-Z]{2}[-~.[:space:]][0-9]{7}

▶ 운전면허번호
[0-9]{2}[-~.[:space:]][0-9]{6}[-~.[:space:]][0-9]{2}

▶ 핸드폰번호
01[016789][-~.[:space:]][0-9]{3,4}[-~.[:space:]][0-9]{4}

▶ 신용카드번호
[34569][0-9]{3}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{4}

▶ 건강보험번호
[1257][-~.[:space:]][0-9]{10}

▶ 계좌번호
([0-9]{2}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{6}|[0-9]{3}[-~.[:space:]]([0-9]{5,6}[-~.[:space:]][0-9]{3}|[0-9]{6}[-~.[:space:]][0-9]{5}|[0-9]{2,3}[-~.[:space:]][0-9]{6}|[0-9]{2}[-~.[:space:]][0-9]{7}|[0-9]{2}[-~.[:space:]][0-9]{4,6}[-~.[:space:]][0-9]|[0-9]{5}[-~.[:space:]][0-9]{3}[-~.[:space:]][0-9]{2}|[0-9]{2}[-~.[:space:]][0-9]{5}[-~.[:space:]][0-9]{3}|[0-9]{4}[-~.[:space:]][0-9]{4}[-~.[:space:]][0-9]{3}|[0-9]{6}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{3}|[0-9]{2}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{7})|[0-9]{4}[-~.[:space:]]([0-9]{3}[-~.[:space:]][0-9]{6}|[0-9]{2}[-~.[:space:]][0-9]{6}[-~.[:space:]][0-9])|[0-9]{5}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{6}|[0-9]{6}[-~.[:space:]][0-9]{2}[-~.[:space:]][0-9]{5,6}).


행정자치부
한국인터넷진흥원

개인정보 수집·제공 동의서 작성 가이드라인

(www.privacy.go.kr>>자료마당>>지침자료)

동의서 작성절차 및 유의사항	관계법령
1 준비 단계	
① 업무처리에 필요한 개인정보 파악	
○ 처리하고자 하는 업무에 꼭 필요한 최소한의 개인정보는 어떤 것들이 있는지 파악합니다. ※ A업무 처리 시(예시) : 성명, 전화번호, 이메일, 주소, 성별, 나이	개인정보 보호법(이하 '법') 제16조제1항
○ 고유식별정보나 민감정보는 일반 개인정보와 구분하여 처리하여야 하므로 처리하고자 하는 개인정보 중에 고유식별정보나 민감정보가 있는지 확인해야 합니다. * 고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호 ** 민감정보 : 사상·신념, 노동조합·정당의 가입·탈퇴. 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력자료 등	법 제23조, 제24조
② 개인정보의 보유기간 확인	
○ 개인정보 처리방침이나 관련 법령 등을 통해 수집·이용할 개인정보의 보유기간을 확인합니다. ○ 일시적인 개인정보 수집·이용 등 보유기간이 따로 명시되어 있지 않다면 업무의 특성을 고려하여 필요최소한의 보유기간을 설정하시면 됩니다.	법 제21조, 제30조
③ 수집·이용에 정보주체의 동의가 필요한지 확인	
○ 개인정보를 수집·이용하기 위해서는 다음 중 어느 하나에 해당하지 않는다면 반드시 정보주체의 동의를 받아야 합니다. **<<동의없이 개인정보 수집·이용이 가능한 경우>>** 1. 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 2. 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우 3. 정보주체와의 계약의 체결 및 이행을 위해 불가피하게 필요한 경우 4. 정보주체 또는 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 ※ 이 경우 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하고, 정보주체에게 개인정보 수집·이용한 사실, 그 사유와 이용내역을 통지 5. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우	법 제15조 제1항

동의서 작성절차 및 유의사항	관계법령
○ 민감정보 또는 고유식별정보*를 처리하기 위해서는 정보주체의 별도 동의가 필요합니다. 다만, 법령에서 민감정보 또는 고유식별정보의 처리를 요구하거나 허용하는 경우에는 동의를 받지 않고 개인정보의 수집·이용이 가능합니다. * 주민등록번호는 법령의 근거가 있거나 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요한 경우에만 수집·이용 가능	법 제23조, 제24조, 제24조의2
○ '정보통신서비스 제공자'인 경우에는 「정보통신망 이용 촉진 및 정보보호에 관한 법률」 제22조제2항에 따라 다음의 어느 하나에 해당하는 경우에는 동의없이 개인정보를 수집·이용할 수 있습니다. **<<동의없이 개인정보 수집·이용이 가능한 경우>>** 1. 정보통신서비스 제공에 관한 계약 이행을 위해 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 3. 다른 법률에 특별한 규정이 있는 경우	정보통신망법 제22조
○ 수집·이용하고자 하는 개인정보의 정보주체가 만14세 미만의 아동인 경우에는 해당 아동의 법정대리인의 동의를 받아야 합니다.	법 제22조 제5항
⑤ 개인정보의 제3자 제공 여부 파악	
○ 개인정보처리자가 수집한 개인정보를 제3자에게 제공하려는 개인정보가 어떠한 것이 있는지 파악합니다. ○ 이 경우 다음의 사항을 확인해야 합니다. **<<제3자 제공시 확인사항>>** 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	법 제17조 제1항
○ 개인정보를 제3자에게 제공하기 위해서는 정보주체의 별도의 동의가 필요합니다. 다만, 다음 각 호 어느 하나의 수집목적 범위에서 제공하는 경우 정보주체의 동의 없이도 가능합니다. **<<동의없이 제3자 제공이 가능한 경우>>** 1. 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 2. 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	법 제17조 제1항

동의서 작성절차 및 유의사항	관계법령
○ 정보통신서비스 제공자도 이용자의 개인정보를 제3자에게 제공하려면 정보주체의 동의가 필요합니다. 다만, 다음 어느 하나에 해당하는 경우에는 동의를 받지 않아도 됩니다. **<<동의없이 제3자 제공이 가능한 경우>>** 1. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 2. 이 법 또는 다른 법률에 특별한 규정이 있는 경우	정보통신망법 제24조의2
○ 개인정보를 국외의 제3자에게 제공할 때에도 정보주체의 동의를 받아야 합니다. **<<개인정보의 국외의 제3자 제공시 확인사항>>** 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용	법 제17조 제3항
○ 제3자 제공하고자 하는 개인정보의 정보주체가 만14세 미만의 아동인 경우에는 해당 아동의 법정대리인의 동의를 받아야 합니다.	법 제22조 제5항
⑥ 개인정보의 수집·이용 및 제3자 제공에 대한 동의 거부시 불이익 검토	
○ 개인정보 수집·이용 및 제3자 제공에 대하여 정보주체가 동의하지 않을 경우 정보주체에게 어떠한 불이익이 있는지 검토합니다. ※ 예시) 고객맞춤형 서비스 제한, 마일리지·포인트 적립 불가 등	법 제15조, 제17조, 제18조
⑦ 개인정보 처리업무 위탁 여부 검토	
○ 개인정보처리자가 개인정보 처리가 수반되는 업무처리를 위탁하고자 할 때에는 별도 동의 없이 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 게재하면 됩니다.	법 제26조
○ 정보통신서비스 제공자는 제3자에게 개인정보 수집·보관·처리·이용·제공·관리·파기 등의 업무를 위탁하는 경우 정보조체에게 위탁을 받는 자와 그 업무내용을 알리고 동의를 받아야 합니다. ※ 다만, 정보통신서비스의 제공에 관한 계약 이행, 정보주체 편의 증진 등을 위하여 필요한 경우로서 개인정보취급방침에 공개하거나 전자우편 등으로 정보주체에게 알린 경우에는 동의를 받지 않아도 됨	정보통신망법 제25조

동의서 작성절차 및 유의사항	관계법령
※ 최초 수집 이후 당초 수집목적의 범위를 벗어나 이용·제공이 필요한 경우	
○ 개인정보를 당초 수집한 목적의 범위를 벗어나 이용하거나 제3자에게 제공하고자 하는 경우 정보주체의 동의를 받아야 합니다. ○ 그러나 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우로서 아래의 어느 하나에 해당하는 경우에는 정보주체의 동의없이 개인정보를 당초 수집한 목적의 범위를 벗어나 이용하거나 제3자에게 제공할 수 있습니다.(다만, 4번~8번은 공공기관에만 해당) 1. 다른 법률에 특별한 규정이 있는 경우 2. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 3. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 제공하는 경우 4. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 5. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 6. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 7. 법원의 재판업무 수행을 위하여 필요한 경우 8. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우	법 제18조
※ 동의를 받은 사항(항목, 목적, 보유·이용 기간 등)을 변경하는 경우 그 사실을 알리고 동의를 받아야 합니다 **※ 개인정보의 목적외 이용·제공 동의서 작성시 유의사항** ○ 업무여건 변화 등으로 인하여 이미 수집·이용 중인 개인정보를 당초 수집 목적의 범위를 초과하여 이용하거나 제3자에게 제공하여야 하는 경우에는 해당하는 정보주체로부터 별도의 동의서를 받아야 합니다. ○ 이 경우 일반 동의서 양식을 그대로 사용하여도 무방합니다.	

2 작성 단계

① 동의서 제목 기재

○ 개인정보 수집·이용에 대한 동의를 받고자 한다는 것을 정보주체가 쉽게 알 수 있도록 동의서 상단에 기재합니다.

※ 예시) ○○회원 가입을 위한 개인정보 수집·이용 동의서,
○○이벤트 참가를 위한 개인정보 수집·이용 동의서

○ 개인정보 수집·이용과 함께 제3자 제공을 하려고 하는 경우에는 이에 대한 동의도 받는다는 것을 명시해야 합니다.

※ 예시) ○○회원 가입을 위한 개인정보 수집·이용 및 제3자 제공 동의서

② 동의서 작성 안내

○ 개인정보 수집·이용(및 제공)에 대한 안내와 동의서 작성 시 정보주체가 주의하여야 할 사항 등을 기재합니다.

※ 예시) ○○회원 가입을 위하여 아래의 개인정보 수집·이용(및 제공)에 대한 내용을 자세히 읽어 보신 후 동의 여부를 결정하여 주시기 바랍니다.

③ 개인정보 수집·이용 내역 기재

○ '준비단계'의 ①, ②번에서 검토된 내용을 바탕으로 개인정보 수집·이용 내역을 아래의 예시를 참고하여 작성합니다.

법 제15조, 제22조 제3항

표준개인정보 보호지침 제13조

< 작성 예시 >

□ 개인정보 수집·이용 내역

항 목	수집목적	보유기간
성명, 전화번호	신제품에 대한 SMS 홍보	1년

④ 동의 거부권 및 동의 거부에 따른 불이익 안내

○ 정보주체는 위 개인정보 수집·이용에 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익 내용을 기재합니다.

※ 예시) 위와 같이 개인정보를 수집·이용하는데 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 일부 서비스 받으실 수 없습니다.

법 제15조 제2항

⑤ 정보주체의 동의여부 확인

○ 정보주체가 개인정보 수집·이용에 동의하는지에 대한 의사를 명확하게 표시할 수 있도록 작성합니다

○ 수집·이용하고자 하는 개인정보의 정보주체가 만14세 미만의 아동이라면 반드시 법정대리인의 동의를 받아야 합니다.

※ 이 경우 법정대리인의 성명, 연락처 등 동의를 받기 위해 필요한 최소한의 개인정보는 법정대리인의 동의 없이 해당 아동으로부터 수집 가능

< 작성 예시 >

위와 같이 개인정보를 수집·이용하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우

위와 같이 개인정보를 수집·이용하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

※ 온라인으로 동의를 받는 경우

위와 같이 개인정보를 수집·이용하는데 동의하십니까?

동의함	□	동의하지 않음	□

* 법정대리인의 동의를 받아야 하는 경우 본인확인 절차를 거쳐 정당한 법정대리인인지를 확인하고 해당 법정대리인이 체크하도록 구현합니다.

법 제15조, 제22조제5항

⑥ 민감정보 처리에 대한 동의여부 확인(필요시)

○ '준비단계' ③번에서 민감정보를 처리하기 위하여 정보주체의 동의가 필요하다고 검토되었다면 아래의 예시와 같이 동의서를 별도로 작성하여야 합니다.

※ 다만, 법령의 근거 등으로 정보주체의 동의가 필요없다고 검토되었다면 아래의 ⑨번에서 그 내용을 안내하시면 됩니다.

○ 정보주체는 위 민감정보 처리에 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익 내용을 기재합니다.

법 제23조, 제22조제5항

< 작성 예시 >

아래와 같이 민감정보를 처리합니다.

항 목	수집목적	보유기간
민감정보 항목 기재	수집목적 기재	보유기간 기재

※ 위와 같이 개인정보를 처리하는데 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 일부 서비스 제공이 제한 될 수 있습니다.

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)
법정대리인 성명 (서명 또는 인)

※ 온라인으로 동의를 받는 경우

위와 같이 민감정보를 처리하는데 동의하십니까?

동의함	□	동의하지 않음	□

* 법정대리인의 동의를 받아야 하는 경우 본인확인 절차를 거쳐 정당한 법정대리인인지를 확인하고 해당 법정대리인이 체크하도록 구현합니다.

⑦ 고유식별정보 처리에 대한 동의여부 확인(필요시)

○ '준비단계' ③번에서 고유식별정보를 처리하기 위해 정보주체의 동의가 필요하다고 검토되었다면 아래의 예시와 같이 동의서를 별도로 작성하여야 합니다.

※ 다만, 법령의 근거 등으로 정보주체의 동의가 필요없다고 검토되었다면 아래의 ⑨번에서 그 내용을 안내하시면 됩니다.

○ 위 고유식별정보 처리에 동의를 거부할 권리가 있다는 사실과 동의 거부에 따른 불이익이 있는 경우 그 불이익 내용을 기재합니다.

법 제24조, 제24조의2, 제22조제5항

○ 고유식별정보중 주민등록번호는 정보주체의 동의를 받아서는 처리할 수 없으며, 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우나 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우에만 처리할 수 있음을 유의하시기 바랍니다.

< 작성 예시 >

아래와 같이 고유식별정보를 처리합니다.

항 목	수집목적	보유기간
고유식별정보 항목 기재	수집목적 기재	보유기간 기재

※ 위와 같이 고유식별정보 처리에 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 일부 서비스 제공이 제한 될 수 있습니다.

위와 같이 고유식별정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우
위와 같이 고유식별정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)
법정대리인 성명 (서명 또는 인)

※ 온라인으로 동의를 받는 경우
위와 같이 고유식별정보를 처리하는데 동의하십니까?

동의함	□	동의하지 않음	□

* 법정대리인의 동의를 받아야 하는 경우 본인확인 절차를 거쳐 정당한 법정대리인인지를 확인하고 해당 법정대리인이 체크하도록 구현합니다.

⑧ 개인정보 제3자 제공 내역 기재 및 정보주체의 동의여부 확인(필요시)

○ '준비단계'의 ⑤번에서 파악된 개인정보 제3자 제공 내역이 '준비단계' ⑥번에서 정보주체의 동의를 받아야 한다고 검토되었다면 아래의 예시와 같이 동의서를 별도로 작성합니다.

○ 정보주체는 위 개인정보 제공에 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익 내용을 기재합니다.

법 제17조, 제18조

< 작성 예시 >

제공 받는자	제공 항목	제공 목적	보유기간
제공받는 자의 명칭	제공하는 개인정보 항목	제공받는 자가 이용하고자 하는 목적	제공받는 자가 보유하는 기간

※ 위와 같이 개인정보를 제공하는데 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 일부 서비스를 제한 받으실 수 없습니다.

위와 같이 개인정보를 제공하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우

위와 같이 개인정보를 제공하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

※ 온라인으로 동의를 받는 경우

위와 같이 개인정보를 제공하는데 동의하십니까?

동의함	□	동의하지 않음	□

* 법정대리인의 동의를 받아야 하는 경우 본인확인 절차를 거쳐 정당한 법정대리인인지를 확인하고 해당 법정대리인이 체크하도록 구현합니다.

⑨ 정보주체의 동의없이 수집·이용하는 개인정보 내역 고지

○ '준비단계' ③번에서 정보주체의 동의없이 개인정보를 수집·이용할 수 있다고 확인된 사항을 예시와 같이 작성합니다.

< 작성 예시 >

개인정보보호법 제15조제1항제3호에 따라 아래와 같이 개인정보를 수집·이용합니다.

개인정보 항목	개인정보 처리사유	수집 근거
해당 개인정보 항목 기재	수집·이용 목적 기재	근거 법령 등 기재

개인정보보호 표준지침 제13조제2항

⑩ 개인정보처리 업무위탁에 대한 동의여부 확인(정보통신망서비스 제공자에 한함)

○ 정보통신망서비스 제공자는 개인정보 처리 업무를 제3자에게 위탁하고자 한다면 위탁받는 자와 그 업무내용을 정보주체에게 알리고 동의를 받아야 합니다. 다만, 정보통신 서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 위 사항을 공개하거나 전자우편 등으로 이용자에게 알린 경우에는 동의 절차를 거치지 아니할 수 있습니다.

정보통신망법 제25조

< 작성 예시 >

당사는 ○○개인정보처리시스템의 유지보수를 위하여 아래와 같이 개인정보처리 업무를 위탁합니다.

취급을 위탁 받는자(수탁업체)	업무내용
[업체명]	위탁업무 기재

위와 같이 개인정보 처리업무를 위탁 하는데 동의하십니까?(예, 아니오)

※ 그 외 개인정보처리자는 위탁자와 위탁하는 업무내용을 홈페이지에 게재하면 됩니다. 홈페이지가 없는 경우에는 그 내용을 사무실에 게시하거나 관보, 주요 일간지, 소식지 등에 게재할 수 있습니다.

붙임 동의서 작성 사례

1 인사/노무

운전직 채용을 위한 개인정보 수집·이용 및 제3자 제공 동의서(예시)

당사는 운전직 직원 채용을 아래와 같이 개인정보를 수집·이용 및 제3자 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ **개인정보 수집·이용 내역**

수집·이용 항목	수집·이용 목적	보유기간
경력, 운전면허번호	채용절차 진행, 경력·자격 확인	「채용공정화에 관한 법률」에 따라 채용 종료후 180일까지

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 채용심사를 할 수 없어 채용에 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ **민감정보 처리 내역**

항 목	수집목적	보유기간
정신질환 여부	운전직 채용 관리	「채용공정화에 관한 법률」에 따라 채용 종료후 180일까지

※ 위의 민감정보 처리에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 채용심사를 할 수 없어 채용에 제한을 받을 수 있습니다.

☞ 위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

□ **고유식별정보 수집·이용 내역**

항 목	수집목적	보유기간
운전면허번호	운전직 채용 관리	「채용공정화에 관한 법률」에 따라 채용 종료후 180일까지

※ 위의 고유식별정보 처리에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 채용심사를 할 수 없어 채용에 제한을 받을 수 있습니다.

☞ **위와 같이 고유식별정보를 처리하는데 동의하십니까?**(예, 아니오)

□ **개인정보 3자 제공 내역**

제공받는자	제공 목적	제공 항목	보유기간
○○계열사	채용절차 진행	학력, 경력	「채용공정화에 관한 법률」에 따라 채용 종료후 180일까지

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 채용심사를 할 수 없어 채용에 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자에게 제공하는데 동의하십니까?** (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

00회사 귀중

2 학교

현장체험학습을 위한 개인정보 수집·이용 및 제공 동의서(예시)

본교는 2015년 ○월 ○○일 실시할 예정인 현장체험학습과 관련하여 아래와 같이 개인정보를 수집·이용 및 제3자에게 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 개인정보 수집·이용 내역

항 목	수집목적	보유기간
학생 : 성명, 학년, 반, 전화번호 학부모 : 성명, 전화번호	현장체험학습 운영	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ 민감정보 처리 내역

항 목	수집목적	보유기간
질병명, 감염 기간, 질병 감염 경로	학생의 위생관리	1년

※ 위의 민감정보 처리에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ **위와 같이 민감정보를 처리하는데 동의하십니까?** (예, 아니오)

□ 개인정보 제3자 제공 내역

제공받는 기관	제공목적	제공하는 항목	보유기간
OO군부대	현장체험학습장 출입자 신분확인	학생의 성명, 학년, 반, 전화번호	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자 제공하는데 동의하십니까?** (예, 아니오)

현장체험학습을 위한 개인정보 수집·이용 및 제공 동의서(예시)

<기타 고지 사항>

개인정보 보호법 제15조제1항제3호에 따라 정보주체의 동의 없이 개인정보를 수집·이용합니다.

개인정보 처리사유	개인정보 항목	수집 근거
학사관리	학생 : 성명, 생년월일, 주소, 보호자 : 성명, 생년월일	「초·중등교육법」 제25조 「학교생활기록의 작성 및 관리에 관한 규칙」

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

00학교장 귀중

3 병원

문자알림서비스 가입을 위한 개인정보 수집·이용, 제공 동의서(예시)

○○병원은 문자알림 서비스 제공을 위하여 아래와 같이 개인정보를 수집·이용 및 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 개인정보 수집·이용 내역

항 목	수집목적	보유기간
성명, 전화번호	예방접종 안내, 최신의학정보	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ 개인정보 제3자 제공 내역

제공받는 기관	제공목적	제공하는 항목	보유기간
00연구소	맞춤형 의학정보 수집	성별, 결혼 여부, 연령, 관심분야	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자 제공하는데 동의하십니까?** (예, 아니오)

<기타 고지 사항>

개인정보 보호법 제15조제1항제2호에 따라 정보주체의 동의 없이 개인정보를 수집·이용합니다.

개인정보 처리사유	개인정보 항목	수집 근거
진료기록부 작성	성명, 생년월일, 주소, 병명	「의료법」 제22조, 동법 시행규칙 제14조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

00병원장 귀중

4 여행업

멤버십 회원 가입을 위한 개인정보 수집·이용 및 제공 동의서(예시)

○○여행사의 멤버십 회원제 운영을 위하여 아래와 같이 개인정보를 수집·이용 및 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ **개인정보 수집·이용 내역**

항 목	수집·이용 목적	보유기간
성명(국문/영문), 연락처	여행상품 및 항공권 예약, 멤버십 마일리지 관리	2년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ **개인정보 3자 제공 내역**

제공받는자	제공 목적	제공 항목	보유기간
○○호텔	숙박시설 정보 제공	관심 여행지, 여행이력	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자 제공하는데 동의하십니까?** (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

○○여행사 귀중

5 건설

홈페이지 회원 가입을 위한 개인정보 수집·이용 및 제3자 제공 동의서(예시)

○○건설사 홈페이지 회원제 운영을 위하여 아래와 같이 개인정보를 수집·이용 및 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ **개인정보 수집·이용 내역**

항목	수집목적	보유기간
성명, 주소, 연락처	신규분양 안내, 건설 동향 정보 제공	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ **개인정보 제3자 제공 내역**

제공기관	수집목적	항목	보유기간
○○건축연구소	맞춤형 건설 동향 정보 수집	생년월일, 결혼여부, 관심지역, 성별	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자 제공하는데 동의하십니까?** (예, 아니오)

년 월 일

본인 성명 (인 또는 서명)

○○건설사 대표 귀중

5 유선방송사

유선방송 가입을 위한 개인정보 수집·이용 및 제공, 위탁 동의서(예시)

○○유선방송의 케이블TV 가입을 위하여 아래와 같이 개인정보를 수집·이용 및 제공, 위탁하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 개인정보 수집·이용 내역

항 목	수집·이용 목적	보유기간
성명, 주소, 연락처	케이블 TV 서비스 제공	2년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 수집·이용하는데 동의하십니까?** (예, 아니오)

□ 개인정보 3자 제공 내역

제공받는자	제공 목적	제공 항목	보유기간
○○리서치	케이블 TV 만족도 조사	성명, 전화번호	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 원활한 서비스 제공에 일부 제한을 받을 수 있습니다.

☞ **위와 같이 개인정보를 제3자 제공하는데 동의하십니까?** (예, 아니오)

□ 개인정보 취급업무 위탁 내역

취급을 위탁 받는자(수탁업체)	업무내용
○○정보통신	케이블TV 신설·폐지, AS 등 유지보수

위와 같이 개인정보 취급업무를 위탁 하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

○○케이블방송사 귀중

공공기관 개인정보 영향평가 수행 시 참고사항

□ 관련 법규

○ 「개인정보 보호법」 제33조(개인정보 영향평가)

○ 「개인정보 보호법 시행령」 제35조(개인정보 영향평가의 대상), 제36조(영향평가 시 고려사항), 제37조(평가기관의 지정 및 지정취소), 제38조(영향평가의 평가기준 등)

○ 「개인정보 영향평가에 관한 고시」(행정자치부 고시 제2015-53호, 2015.12.31.)

□ 영향평가 개요

○ (목적) 개인정보를 처리하는 시스템을 구축 또는 변경하는 경우 위험요인을 분석하고 개선사항을 도출하여 개인정보 침해사고 예방

○ (대상) 개인정보 처리 시스템을 구축 또는 변경하려는 공공기관

<영향평가 수행 대상 : 개인정보 보호법 시행령 제35조>

- 5만 명 이상의 민감정보 또는 고유식별정보가 포함된 개인정보파일
- 공공기관 내부 또는 외부 개인정보파일과 연계 결과 50만 명 이상의 개인정보가 포함된 개인정보파일
- 100만 명 이상의 개인정보가 포함된 개인정보파일
- 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분

○ (평가기관) 행정자치부장관이 지정한 18개 기관

※ 개인정보보호 종합포털(www.privacy.go.kr) 사업자 > 개인정보 영향평가 > 영향평가 안내 > 평가기관목록에서 확인 가능

□ 영향평가 수행 시기

○ 신규 시스템 구축 또는 기존 시스템 변경 시 시스템 분석·설계 단계

○ 시스템 운영 중 중대한 개인정보 침해위험 발생 우려 시

○ 개인정보 보호법 시행령 시행(2011.9.30.) 전 구축·운영 시스템은 '16.9.까지 수행

※ 개인정보 보호법 시행령(2011.9.30.) 부칙 제6조(개인정보 영향평가에 관한 경과조치) 참조

□ 영향평가 사업 담당자 유의사항

○ 투입인력의 영향평가 수행 자격 확인(인증서 확인)

※「개인정보 영향평가에 관한 고시」에 따라 제5조에 따라 전문인력 인증을 받은 경우 영향평가 수행 가능

○ 영향평가는 시스템 구축·운영 전 개인정보 침해 요인을 찾고, 이를 개선하여 개인정보 침해사고를 예방하는 것이 목적이므로

- 영향평가기관이 영향평가 사업 발주기관과 관련 시스템을 정확히 이해할 수 있도록 자료 제공 등에 적극 협조하고

- 기관과 시스템의 특성을 반영한 개선사항 도출 등 내실 있는 영향평가 사업이 될 수 있도록 관리·감독 철저

○ 개인정보보호종합지원시스템(intra.privacy.go.kr)에 영향평가 결과 등록

- 영향평가서 : 사업 완료 후 2개월 이내

- 개선계획 이행점검 확인서 : 사업 완료 후 1년 이내

□ 참고자료

○ 개인정보 영향평가 수행안내서

※ 개인정보보호 종합포털(www.privacy.go.kr) 사업자 > 개인정보 영향평가 > 영향평가 자료실에서 다운로드 가능

개정 「개인정보보호법」 시행('14.8.7.)에 따른

주민등록번호 수집 금지 제도 가이드라인

2014. 1.

안 전 행 정 부
개인정보보호과

목 차

Ⅰ. 개요 ····· 1

Ⅱ. 주민번호 수집·이용 현황 ····· 2

Ⅲ. 개선 방향 ····· 4

Ⅳ. 주민번호 수집 금지에 따른 조치사항 ····· 5

1. 기본 원칙 ····· 5

2. 판단 기준 ····· 5

3. 주민번호 수집 금지 체크리스트 ····· 7

4. 개선 절차 ····· 8

5. 기관별 조치사항 ····· 9

Ⅴ. 지원 체계 ····· 10

【붙임】

1. 주민번호 처리 근거 법령 정비 입법례

2. 입법 모델 및 참고사항

3. 주민번호 수집 금지 필요성 검토 및 조치사항 예시

4. 주민번호 미수집 전환 시범 사례

5. 주민번호 수집·이용 허용 법령 사례

6. 주민번호 수집 금지 정책 관련 Q&A

Ⅰ 개 요

1 배경

○ **주민번호 수집 원칙적 금지, 유출시 과징금 부과** 등을 주요 내용으로 **개인정보보호법 개정 (공포 '13.8.6일, 시행 '14.8.7일)**

- 이에 따라, '14.8.7일부터 **법령상 근거 없이** 불필요하게 **주민번호를 수집하는 행위가 엄격히 제한** (위반시 과태료 부과)

※ 온라인상 주민번호 수집 금지 제도는「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에 따라 '12. 8월부터 旣 시행 중

<주민번호 수집 금지 정책 추진 경과>

⇨ '12.4월 : '주민번호 수집이용 최소화 종합대책' 마련(안행부, 방통위, 금융위 참여)
⇨ '12.8월 : 정보통신서비스제공자 등 온라인상 주민번호 수집 금지 시행(방통위)
⇨ '14.8월 : 오프라인 및 공공기관 등 주민번호 수집 금지 시행 예정(안행부)

2 개정「개인정보보호법」주요 내용

○ **'주민번호 수집 법정주의' 신설** (제24조의2)

- **주민번호 처리를 원칙적으로 금지**하고, 아래 사유에 해당하는 **예외적인 경우**에만 **허용** (위반시 3천만원 이하 과태료 부과)

< 주민번호 예외적 처리 허용 사유 >

1. 법령(법률·시행령·시행규칙)에서 구체적으로 주민번호 처리를 요구·허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우
3. 기타 주민번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

- 기 보유한 주민번호는 **법 시행 후 2년 이내('16.8.6일까지) 파기**

○ **주민번호 유출에 대한 '과징금 제도' 신설** (제34조의2)

- 주민번호 유출 등이 발생한 경우로서 안전성 확보조치를 하지 않은 경우 **최대 5억원 이하의 과징금** 부과·징수

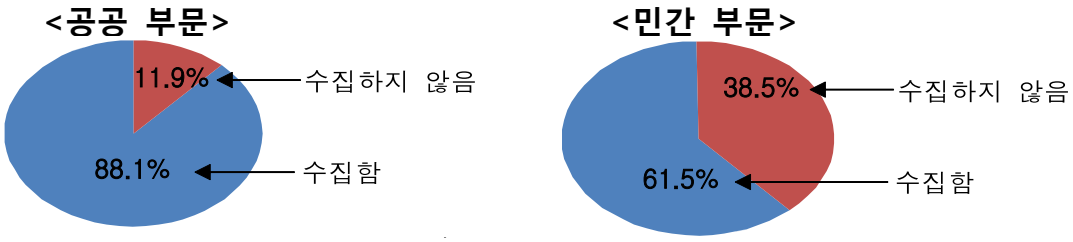
○ **대표자(CEO)** 등에 대한 **징계권고 신설** (제65조제3항)

- 법규위반행위에 따른 안전행정부장관의 **징계 권고 대상에 대표자(CEO)** 및 책임있는 임원이 **포함됨을 명시**

Ⅱ 주민번호 수집·이용 현황

○ **주민번호**는 행정, 금융, 의료, 복지 등 **사회 전 분야**에서 **개인식별을 위한 기초 자료**로 널리 활용(공공 88.1%, 민간 61.5%가 주민번호 수집)

- **(공공)** 법령상 의무 준수(54.6%), 본인 확인(50.3%) 등을 위해 수집
- **(민간)** 본인 확인(54.8%), 계약 체결 및 이행(37.8%) 등을 위해 수집

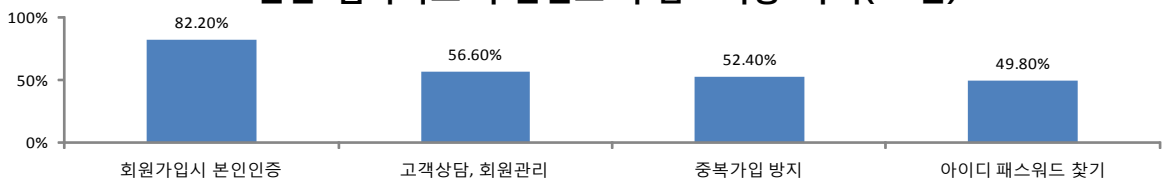


※ 출처 : 2013 개인정보보호 실태조사(안전행정부, 개인정보보호위원회)

○ 주민번호 수집이 반드시 필요하지 않음에도 **관행적으로 과다 수집·이용하는 빈도**가 매우 높음

- 주민번호를 수집·이용하는 국내 웹사이트(약 32만개) 중 **92.5%(약 29.6만개)가 불필요한 수집**('13.4월, 국회입법조사처 검토보고서)
- **공공기관 50.3%, 민간사업자 54.8%**가 **단순 본인확인 목적**으로 주민번호 수집(2013 개인정보보호 실태조사, 안행부·개인정보보호위원회)

< 민간 웹사이트 주민번호 수집·이용 목적('12년) >



※ 출처 : 2012년 정보보호 실태조사(KISA, '12.12월)

< 시 사 점 >

◎ 주민번호는 **사회 전 분야에서 널리 활용**되고 있으나 웹사이트 회원관리, 단순 본인확인 등 **불필요하게 수집하는 경우가 많음**

⇒ **유출·오남용 등에 따른 위험성***을 고려할 때, 불필요한 주민번호 요구 관행의 시급한 개선 필요

* 유출 사례 : S사 3,500만건('11.7월), N사 1,320만건('11.11월), K사 870만건('12.7월) 등

【참고 1】 해외 주요국의 고유식별정보 제도

□ 우리나라의 주민번호와 같이 해외 주요국가에서도 국민식별정보, 사회보험번호, 사회보장번호 등 고유식별정보를 사용 중

○ 사용 목적 및 범위를 특정하는 등의 조치를 통해 불필요한 활용 제한

구분	세부내용
미국	▶ **사회보장번호**(Social Security number: SSN)를 사용함 - Privacy Act of 1974 에 SSN 요구시 제출의 필수성 여부, 요구의 법률근거, 제공된 SSN의 사용목적 및 제시거부 등의 처리방법 사전 고지 ▶ 개별 법률에서 번호의 이용 및 보호에 관한 규정을 두고, 문제 발생 시 그 책임의 소재에 관한 규정까지 포함
영국	▶ 국민건강보험서비스(the National Health Service: NHS) 등록 시 **개인식별번호** 부여
캐나다	▶ **사회보험번호**(SIN : Social Insurance Number)를 사용함 ▶ 벌금부과, 소득세 징수, 실업급여 등 15개 행정업무에만 사용 ▶ 법률 규정이 없는 경우 사회보험번호 수집 등 행위가 프라이버시 침해를 상회하는 사회적 이득이 있는 경우만 수집·사용 가능 ▶ 사회보험번호 제시를 요구하는 경우 개인에게 그 목적, 강제성 여부, 제시 거부시의 결과 등을 사전 고지하여야 함
스웨덴	▶「개인정보보호법(Personal Data Act 1998 : 204)」 '민감한 개인정보(sensitive personal data)'에 **국민식별번호**를 포함 ▶ (제22조) 처리 목적, 신원보안의 중요성, 기타 중요한 사유 외에 본인의 동의 없이 개인식별번호를 사용할 수 없음 ▶ (제50조) 정부 또는 정부가 지명한 기관으로 하여금 개인식별번호를 사용할 수 있는 범위를 특정하도록 하고 있으며,감독 당국의 결정은 규정에 관련된 경우가 아니라면 일반행정법원에 항소할 수 있음

※ 참조 : "국내 개인정보보호법의 발전방향 제시를 위한 국외 개인정보보호법 분석" 정보보호학회 논문지, 2012.10.

Ⅲ 개선 방향

1 목표 : 사회 전 분야 주민번호 미수집 환경 구축

2 개선 방향

▸ **법 시행일('14.8.7.) 이후 사회 전반의 불필요한 주민번호 수집 금지**
⇒ 대체수단 도입 등을 통해 주민번호 수집 금지 추진

▸ **주민번호 수집을 요구하는 업무 전반 파악, 법제도 · 서식 등 개선 추진**
⇒ 관련 법제도, 내부 규정, 업무절차, 관련 서식 정비 등 병행

○ 개정「개인정보보호법」에 따라 '14.8.7일부터 **모든 공공기관 및 민간사업자** 등 사회 전 분야의 불필요한 **주민번호 수집 금지**

- 법령상 근거가 없는 경우에는 대체수단 도입 등을 통해 주민번호를 수집하지 않도록 하고, 기 보유한 주민번호는 **'16.8.6일까지 파기**

※ 주민번호 수집을 요구하는 업무절차, 내부규정, 서식 개선 등 병행

○ 주민번호 수집이 불가피한 경우에는 **해당 소관부처를 통해 법령 근거 마련** 및 **필요 최소한 범위 내 주민번호 수집 · 이용**

- 민간사업자/협회, 소관부처 등은 소관업무와 관련한 주민번호 수집 필요성을 검토하고 불가피한 경우에 한하여 법령 근거* 마련

* **[붙임1] 주민번호 처리 근거 법령 정비 입법례 참조**

Ⅳ 주민번호 수집 금지에 따른 조치사항

1 기본 원칙

1. 법령상 구체적 근거가 있는 경우에는 현행 유지
2. 법령상 근거는 없으나 주민번호 수집이 불가피한 경우 법령 근거 마련
   ▸ (민간사업자/협회) 해당 업종 소관부처에 법령 근거 마련 지원 요청
   ▸ (소관부처) 타당성 검토 후 불가피한 경우에 한하여 법령 근거 마련
3. 위 1, 2에 해당하지 않는 경우 주민번호를 수집하지 않도록 전환

2 판단 기준

○ 모든 개인정보처리자는 아래 판단 기준에 따라 **주민번호 수집 금지 필요성을 검토**하고 그에 따른 **조치사항을 이행**

<기준 1> 주민번호 처리 법령 근거 유무

- **법령(법률, 시행령, 시행규칙)상** 주민번호 수집을 구체적으로 **허용하는 경우***에는 **현행 유지**

  * **[붙임1] 주민번호 처리 근거 법령 정비 입법례 참조**

(예시) 법령 조문에서 주민번호 수집을 요구·허용하는 경우, 법정 서식에서 주민번호 기재란이 있는 경우, 법령 조문 또는 서식상 주민번호가 포함된 서류(주민등록등·초본 등)를 수집할 수 있도록 허용 하는 경우 등을 말함

- 법령상 근거가 없는 경우 아래 <기준 2> 검토에 따른 조치사항 이행

<기준 2> 불가피성 유무(주민번호 대체 불가능성)

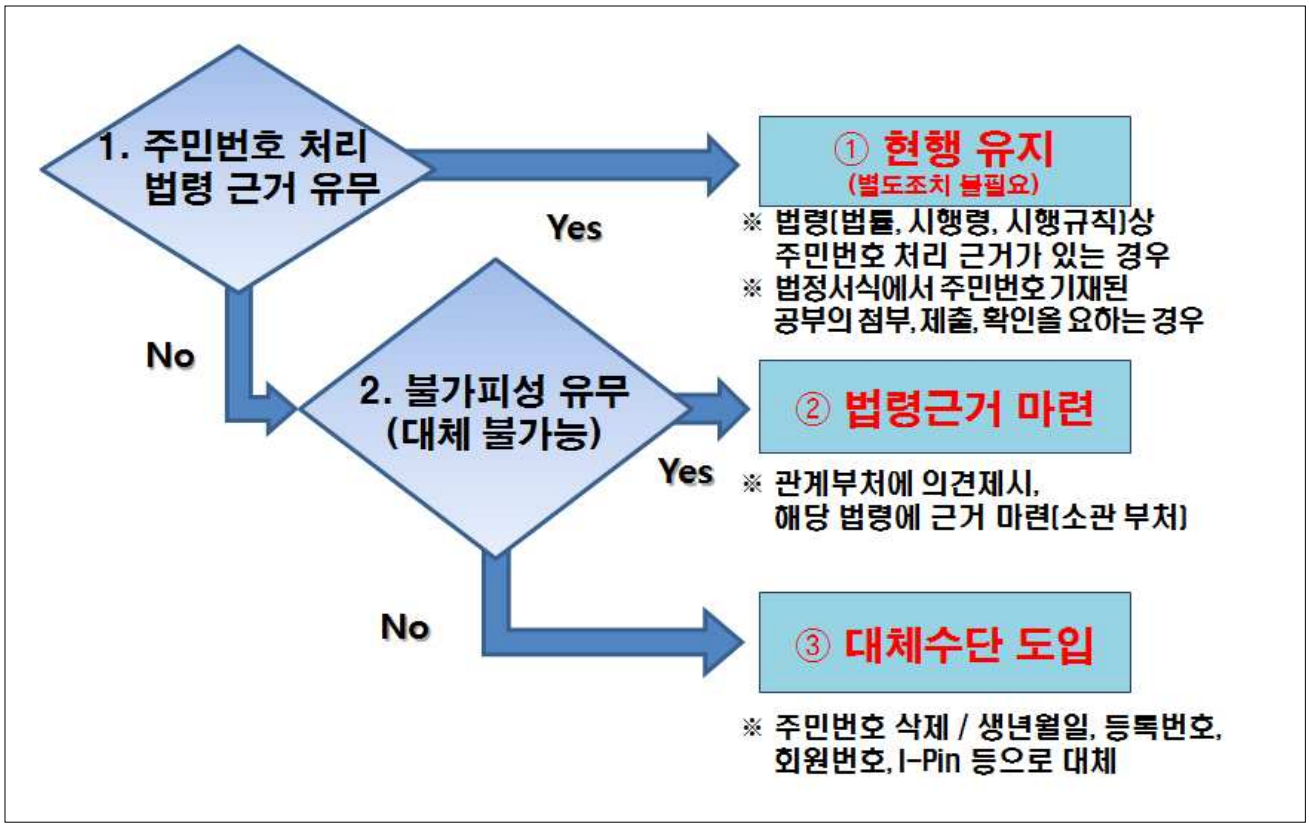
- 법령상 근거는 없으나 반드시 주민번호를 수집하여야 할 필요가 있는 경우 해당 업무 **소관부처를 통해 법령근거* 마련**

  * **[붙임2] 법령근거 마련을 위한 입법 모델 및 참고사항 참조**

- 주민번호 수집 필요성이 없거나 대체 가능한 경우에는 전화번호 등 다른 수단으로 대체하고, 기 보유 주민번호는 파기

(예시) 단순 본인확인을 위한 경우, 회원DB 관리를 위한 Key 값으로 활용하는 경우 등은 주민번호 수집 필요성이 낮으며 다른 수단으로 대체 가능한 경우에 해당

【참고 2】 주민번호 수집 금지 판단 기준



① (기준 1→ Yes) 법령상 구체적 주민번호 처리 근거가 있는 경우

▸ **현행 법령**에서 정한 바*에 **따라 주민번호 처리**(별도 조치 불필요)

* 「금융실명거래법」에 따른 금융기관의 실명거래, 「의료법」에 따른 의료기관의 진료기록부 작성 등은 법령상 주민번호 처리 근거가 있는 경우에 해당

② (기준 1→No, 기준 2→ Yes) 법령상 근거는 없으나 주민번호를 수집하지 않을 경우 근본적으로 해당 업무 수행이 불가능한 경우

▸ 해당 업무 소관부처에 **법령 근거 마련을 요청**

③ (기준 1→No, 기준 2→ No) 법령상 근거가 없으며 주민번호를 반드시 수집하여야 할 필요성도 없는 경우

▸ 주민번호를 수집하지 않거나 전화번호, 생년월일, *i*-PIN 등 **다른 수단으로 대체**(관련 업무규정 및 절차, 서식 개선 등 병행), 기 보유 주민번호는 파기

※ 급박한 재해, 재난 상황 등 '정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 명백히 필요하다고 인정되는 경우'에는 개인정보보호법 제24조의2제1항제2호에 따라 별도의 법령 근거 없이 주민번호 처리 가능

3 주민번호 수집 금지 체크리스트

○ 주민번호 수집 금지 필요성을 점검하고 그에 따른 조치사항을 파악할 수 있는 체크리스트는 아래와 같음

- 구체적인 상황별 검토 결과 사례는 [붙임 3] 참조

<table>
<tr><th colspan="3" rowspan="2">점검사항</th><th colspan="2">점검결과</th></tr>
<tr><th>예</th><th>아니오</th></tr>
<tr><td rowspan="2">점검
단계</td><td>1. 주민번호 수집
법령근거 유무</td><td><u>현재 주민번호를 수집하고 있는 업무가 법령에 근거를 두고 있는가?</u>
* ‘법령’은 법률, 시행령, 시행규칙을 의미함
* 행정규칙(고시, 훈령) 및 지방자치단체의 조례 등은 개인정보보호법 제24조의2에 따른 ‘법령’에 해당하지 않음
* ‘법령’의 별지 서식에 ‘주민번호 기재항목’이 있거나, 주민번호가 기재된 서류의 제출, 첨부 등을 규정한 경우에도 법령 근거가 있는 것으로 봄
* ‘처리’란 수집·이용, 기록, 저장 등 제반 행위를 의미</td><td></td><td></td></tr>
<tr><td>2. 불가피성 유무
(대체가능성)</td><td><u>해당 업무수행을 위해서는 주민번호 수집이 불가피한가?</u>
* ‘불가피성’이란 주민번호를 수집하지 않으면 그 해당업무의 수행이 근본적으로 불가능한 경우를 의미
* 전화번호, 생년월일, I-PIN 등 대체수단을 적용하거나 다른 개인정보 항목(예컨대 성명+생년월일 등)으로 대체하여도 업무에 지장이 없다면 ‘불가피성‘이 없는 것임</td><td></td><td></td></tr>
<tr><td colspan="2">조치사항</td><td colspan="3">
<table>
<tr><th>구분</th><th>법령근거</th><th>불가피성</th><th>조치사항</th></tr>
<tr><td>①</td><td>있음</td><td></td><td>별도 조치 불필요 (현행 유지)</td></tr>
<tr><td>②</td><td>없음</td><td>있음</td><td>법령 근거 마련</td></tr>
<tr><td>③</td><td>없음</td><td>없음</td><td>주민번호 삭제,
생년월일 등으로 전환,
I-PIN 등 대체수단 도입</td></tr>
</table>
</td></tr>
</table>

④ 개선 절차

<주민번호 수집 금지 개선단계 및 일정>

STEP 1		STEP 2		STEP 3
주민번호 처리 실태 자체조사, 수집 금지 필요성 검토, 필요시 법령근거 마련 요청	➪	주민번호 수집 금지 계획 수립 및 시행	➪	기 보유 주민번호 파기
'14.3월말 이전까지		'14.8.7일 이전까지		'16.8.6일까지

○ **(Step 1) 자체적 실태조사·분석 및 수집 금지 필요성 검토**

- 민간사업자, 공공기관 등 모든 개인정보처리자는 소관 업무 수행과 관련한 주민번호 처리실태 자체 조사 및 수집 금지 필요성 검토
- 주민번호 수집이 불가피한 경우에는 해당 소관부처에 법령 근거 마련을 요청(입법 소요기간을 고려하여 '14.3월까지 법령 정비 요청)

※ '12.1월~'13.1월 중 27개 부처 299개 법령에 주민번호 처리 근거 일괄 정비 완료

* (예시) 주민번호 미수집시 법령상 의무 이행이 불가능하거나, 정보주체 또는 제3자의 부당한 이익 침해가 예상되는 경우 등은 불가피한 경우에 해당

○ **(Step 2) 주민번호 수집 금지 계획 수립 및 시행**

- 당해 업무 특성 및 연계 서비스 현황 등을 종합적으로 고려하여 주민번호 수집 금지를 위한 대체수단 도입 등 구체적 계획 수립
- 주민번호를 요구하는 업무절차, 내부규정, 서식 등 개선 병행*

* **(붙임 4) 주민번호 미수집 전환 시범 사례 참조**

○ **(Step 3) 기 보유 주민번호 파기**

- 법령상 주민번호 수집 근거가 없는 경우 '14.8.7일 이전까지 미수집 전환을 완료한 후, 기 보유 주민번호는 '16.8.6일까지 모두 파기
- 단, 계약 또는 거래 등과 관련하여 수집한 주민번호는 당사자간 권리 의무 관계에 미치는 영향, 관련 법령 정비 추이 등을 충분히 고려하여 신중히 파기

5 기관별 조치사항

○ 중앙행정기관

- 법령, 행정규칙(훈령·예규·고시 등), 행정서식, 민간서식 등을 통한 주민번호 처리 실태 조사·분석 (소관분야 관련 공공 및 민간 총괄)
- 주민번호 수집 필요성 및 수집 금지 타당성 검토(지방자치단체, 민간협회/단체 등 이해관계자 의견 수렴 및 반영)
- 주민번호 수집이 불가피한 경우 관련 법령근거 정비, 불필요한 경우 대체수단 도입 등 미수집 전환 추진(하위규정 및 서식 등 개선 병행)

○ 지방자치단체, 기타 공공기관

- 관련 법령, 조례, 자체 지침 및 규정, 관련 서식 등을 통한 주민번호 처리 실태 조사·분석 (소관업무 관련 공공 및 민간 총괄)
- 주민번호 수집 필요성 및 수집 금지 타당성 검토(관련 중앙행정기관, 기초자치단체, 산하기관, 민간협회/단체 등 이해관계자 의견 수렴 및 반영)
- 주민번호 수집이 불가피한 경우 관계 중앙행정기관 협의 및 의견제시, 불필요한 경우 대체수단 도입 등 미수집 전환 추진(업무절차 및 서식 등 개선 병행)

○ 민간사업자, 협회/단체

【민간사업자】

- 소관 사업과 관련한 주민번호 처리 실태, 주민번호 수집 금지에 따른 고객서비스 및 영업상 영향도 등 조사·분석
- 주민번호 수집이 불가피한 경우 관련 협회/단체 등을 통해 관계 중앙행정기관에 법령근거 마련 요청, 불필요한 경우 미수집 전환 추진(내부 규정, 고객관리프로그램, 서비스 신청서식 등 개선 병행)

【협회/단체】

- 소관 업종에 종사하는 민간사업자 의견 수렴 및 관계 중앙행정기관 의견 제시, 주민번호 수집 금지 정책 및 지원체계* 적극 안내

※ 본 가이드라인 10쪽, 'Ⅴ. 지원체계' 참조

Ⅴ 지원체계

○ **법령 근거 마련 지원**

- **(각 중앙행정기관)** 소관분야 이해 관계자(민간협회/단체 등) 의견수렴을 통해 주민번호 수집이 불가피한 경우에 한하여 법령 근거 마련 지원

- **(안전행정부)** 각 중앙행정기관을 대상으로 주민번호 수집 근거 마련을 위한 입법례, 법령 반영 필요성 검토 사항 등 지원

○ **상담 및 컨설팅 지원**

- 전담창구 운영을 통한 법제도·기술지원 등 상담 및 컨설팅 제공

※ 한국인터넷진흥원 내 '주민번호 전환 지원 전담반' 운영

<주민번호 전환 지원 전담반 연락처>

◇ 대표 문의처 : 국번 없이 118번

◇ 관련 법제도 상담 및 컨설팅 문의

☞ 이메일 : jumin@kisa.or.kr

◇ 대체수단 도입 등 기술지원 상담 및 컨설팅 문의

☞ 이메일 : privacy_support@kisa.or.kr

※ 기타 문의

- ▸ 공공아이핀 : 공공아이핀센터(02-818-3050)
- ▸ 민간아이핀 : NICE 아이핀(1588-2486), SIREN24(1577-1006)
- ▸ 관련 자료 : 개인정보보호종합지원포털(www.privacy.go.kr > 자료실)

붙임 1 주민번호 처리 근거 법령 정비 입법례

○ '12.1 ~ '13.1월 중 27개 부처 소관 299개 대통령령 일괄정비 입법례

법령 명	조문 내용
과세자료의 제출 및 관리에 관한 법률 시행령 (2012.1.6. 개정)	제6조(민감정보 및 고유식별정보의 처리) ① 「국세기본법」 제2조제17호에 따른 세무공무원은 법 및 이 영에 따른 과세자료의 제출 및 관리에 관한 사무를 수행하기 위하여 불가피한 경우 법 제6조부터 제8조까지의 규정에 따라 제출받은 「개인정보 보호법」 제23조에 따른 건강에 관한 정보나 같은 법 시행령 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. ② 과세자료제출기관의 장은 법 제6조부터 제8조까지의 규정에 따라 과세자료를 제출하기 위하여 불가피한 경우 제1항에 따른 개인정보가 포함된 자료를 처리할 수 있다.
취업 후 학자금 상환 특별법 시행령 (2012.1.6. 개정)	제45조의2(고유식별정보의 처리) 교육과학기술부장관(법 제5조에 따라 교육과학기술부장관의 권한을 위임·위탁받은 자를 포함한다)은 법 및 이 영에 따른 취업 후 상환 학자금대출, 그 상환 및 관리 등에 관한 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다.
병역법 시행령 (2012.1.6. 개정)	제157조(민감정보 및 고유식별정보의 처리) ① 국방부장관은 제118조의3 및 제119조의3에 따른 군종·의무·수의 분야 현역 장교의 선발에 관한 사무와 제119조에 따른 군종사관후보생 선발에 관한 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다. ② 병무행정관서의 장은 법에서 정한 병역의무자의 제1국민역 편입, 징병검사(재징병검사를 포함한다), 징집, 모집, 소집, 입영, 복무 및 전역 등 병무행정에 관한 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보 또는 같은 법 시행령 제18조

	제2호에 따른 범죄경력자료에 해당하는 정보나 같은 영 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. ③ 법 제80조제2항에 따른 병무행정에 대한 협조 또는 법 제81조제2항 후단에 따른 자료제공을 요청받은 기관의 장은 그 협조 또는 자료제공을 위하여 불가피한 경우 제2항에 따른 개인정보가 포함된 자료를 처리할 수 있다.
국적법 시행령 (2012.1.6. 개정)	제30조(민감정보 및 고유식별정보의 처리) 법무부장관(제29조에 따라 법무부장관의 권한을 위임받은 자를 포함한다) 또는 사무소장등은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 사상·신념, 정치적 견해, 건강에 관한 정보, 같은 법 시행령 제18조제1호 또는 제2호에 따른 유전정보 또는 범죄경력자료에 해당하는 정보, 같은 영 제19조제1호·제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. 1. ~ 8. (생략)
전통시장 및 상점가 육성을 위한 특별법 시행령 (2013.1.16. 개정)	제34조의2(고유식별정보의 처리) 중소기업청장(법 제71조에 따라 중소기업청장의 권한을 위임·위탁받은 자를 포함한다)은 법 제26조제3호에 따른 공동상품권의 발행에 관한 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제2호에 따른 주민등록번호 또는 여권번호가 포함된 자료를 처리할 수 있다.
특정금융거래정보의 보고 및 이용 등에 관한 법률 시행령 (2013.1.16. 개정)	제16조(민감정보 및 고유식별정보의 처리) 금융정보분석원장(법 제11조제6항에 따라 금융정보분석원장의 권한을 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 자료, 같은 영 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호가 포함된 자료를 처리할 수 있다. 1. ~ 7. (생략)

※ 정비 대상 법령이 다수인 경우에는 일괄개정 입법례*를 참조하여 부처별 일괄 정비 가능

* (예시) 「민감정보 및 고유식별정보 처리 근거 마련을 위한 과세자료의 제출 및 관리에 관한 법률 시행령 등 일부개정령」(대통령령 제23488호, 2012.1.6일 공포) 등

붙임 2 입법 모델 및 참고사항

【입법모델 1】: 주민번호 처리가 필요한 사무가 다수인 경우

제00조[1](고유식별정보의 처리) ○○○장관 (제00조에 따라 ○○○장관의 권한을 위임·위탁받은 자를 포함한다)은[2] 다음 각 호의 사무[3]를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 시행령 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제0조제0호에 따른 ○○○사무
2. 법 제00조제00호에 따른 ○○○사무
3. 제1호부터 제2호까지의 규정에 따른 사무를 수행하기 위하여 필요한 사무

【입법모델 2】: 주민번호 처리가 필요한 사무가 1~2개인 경우

제00조[1](고유식별정보의 처리) ○○○장관 (제00조에 따라 ○○○장관의 권한을 위임·위탁받은 자를 포함한다)은[2] 법 제00조에 따른 ○○○사무[3] 및 이 영 제00조에 따른 ○○○사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 시행령 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다.

【참고사항】

1) 규정의 위치는, 원칙적으로 보칙의 장·절, 또는 이에 상당하는 위치에 신설하되, 특별한 사정이 없으면 권한의 위임·위탁 규정 다음, 벌칙 규정 전에 적절한 위치에 신설(단, 현행 조문을 보완하는 경우에는 '항;으로 신설 가능)

2) 법령상 행정권한 또는 업무가 위임·위탁된 경우로서 그 사무를 처리하기 위해 주민번호를 처리할 필요가 있는 경우 위 괄호와 같이 규정

3) 주민번호 처리가 필요한 사무를 구체적으로 열거하여 규정하고, 일관성 유지를 위하여 "○○○업무" 대신 "○○○사무"로 통일하여 사용. 다만, 해당 법령규정 전체의 맥락에서 보다 적합한 용어가 있는 경우에는 해당 용어를 사용함.

※ 업무 특성상 주민번호 외 운전면허번호, 여권번호 등 다른 고유식별정보의 처리도 필요한 경우에는 필요한 정보를 추가로 기재('국가법령정보센터'(www.law.go.kr) > 조문제목 > '고유식별정보' 검색 결과 참조)

※ 법령 상에서 단순히 '신원확인' 또는 '연령확인' 등의 의무만을 규정하고 있다면 주민번호 처리근거를 구체적으로 규정한 경우라 볼 수 없으므로, 상기의 【입법모델】 등과 같이 구체적 근거 규정을 신설하여야 함

붙임 3 주민번호 수집 금지 필요성 검토 및 조치사항 예시

<사례 1> 금융실명거래 제도		
검토	① 법령근거 유무	**있음** ⇒ 「금융실명거래 및 비밀보장에 관한 법률」 제3조 ※ 주민등록증, 주민등록표등본 등으로 실지명의 확인
	② 불가피성 유무	**있음** ⇒ 주민번호 미처리시 금융실명거래 제도 유지 곤란
결론 및 조치사항		별도 조치 불필요 (현행 주민번호 처리 유지)

<사례 2> 원천징수영수증 발급		
검토	① 법령근거 유무	있음 ⇒「소득세법」 제145조·제164조, 동법 시행령 제193조 및 제213조 등 ※ 원천징수의무자 등 주민번호 기재 명시
	② 불가피성 유무	있음 ⇒ 주민번호 미처리시 원천징수의무자에 대한 신고업무 곤란
결론 및 조치사항		별도 조치 불필요 (현행 주민번호 처리 유지)

<사례 3> 홈페이지 회원 가입·관리		
검토	① 법령근거 유무	없음 ⇒ 단순 회원관리를 위한 주민번호 처리는 법령근거 없음 ※ 게시판 본인확인을 규정한 舊 정보통신망법 제44조의5는 헌법재판소에서 위헌판결로 효력 상실 ※ 다만 전자상거래업자 등의 경우 거래기록 보존을 위해 주민번호 처리 가능(「전자상거래 등에서의 소비자 보호에 관한 법률 제6조제2항)
	② 불가피성 유무	없음 ⇒ 생년월일+전화번호 조합, i-PIN 등으로 대체 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입

<사례 4> 사회적 배려 대상자에 대한 공공요금 경감 (가스, 전기, 수도 등)		
검토	① 법령근거 유무	없음 ⇒ 다만 개별 지침 또는 고시 등에서 주민번호 처리근거를 두는 경우가 존재 ※ '도시가스요금 경감지침'(산업통상자원부 지침), '보편적 역무 손실보전금 기준'(미래창조과학부 고시) 등에서 장애인등 요금감면시 주민번호 요구
	② 불가피성 유무	있음 ⇒ 요금감면 대상자의 정확한 신원확인·조회 및 부정 수급·혜택 방지 등을 위해 주민번호 처리 필요
결론 및 조치사항		해당 법령 개정 필요 (관계 공기업, 사업자 등은 소관 중앙행정기관과 협의 및 의견제시)

<사례 5> 직원 신규 채용시 신상기록·명부 기재		
검토	① 법령근거 유무	있음 ⇒「국민건강보험법」등 공적보험 처리, 「근로기준법」 제42조 및 동법 시행령 제22조에 따른 임금대장 작성, 「소득세법」에 따른 소득세 원천징수 등을 위한 주민번호 처리근거 존재
	② 불가피성 유무	있음 ⇒ 근로계약 체결 및 관계 법령에서 요구하는 기재사항의 작성을 위해 주민번호 처리 필요
결론 및 조치사항		별도 조치 불필요 (현행 주민번호 처리 유지) ※ 단, 채용전형 진행단계에서는 주민번호가 불필요하므로 생년월일 등으로 대체하여야 하며, 최종합격자에 한해 주민번호 수집·이용 (인사·노무분야 개인정보보호 가이드라인 참조)

<사례 6> 온라인 실명확인 서비스		
검토	① 법령근거 유무	없음 ⇒ 개별 법령에 연령확인의무 또는 본인확인의무 규정이 있더라도 '주민번호' 이용 근거가 구체적으로 규정되지 않으면 '이름+주민번호' 방식의 실명확인 불가
	② 불가피성 유무	없음 ⇒ i-PIN, 휴대전화, 공인인증서 등으로 대체 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입

<사례 7> 임직원 단체보험 가입		
검토	① 법령근거 유무	있음 ⇒ 보험업법 시행령상 단체보험 가입 등을 위한 필요한 경우 피보험자 주민번호를 처리할 수 있는 명시적 규정 존재
	② 불가피성 유무	있음 ⇒ 단체보험 계약체결시 보험계약 당사자인 회사는 피보험자인 임직원의 주민번호를 수집하여 보험회사에 전달 필요
결론 및 조치사항		별도조치 불필요 (현행 유지) ※ 단 보험가입을 위해 새로 수집한 주민번호는 보험회사 전달 후 즉시 파기 필요

<사례 8> 멤버십 회원 본인확인 (대형마트, 백화점 등)		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 성명+휴대전화번호 등의 조합으로 대체 가능
결론 및 조치사항		주민번호 삭제 및 다른 정보 조합으로 대체

<사례 9> 렌터카 이용 계약시 주민번호 처리		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 운전면허번호로 대체 가능
결론 및 조치사항		주민번호 삭제 및 다른 고유식별정보로 대체 ※ 단 보험가입을 위해 필요한 경우는 주민번호 처리가능

<사례 10> 호텔 등 숙박시설 이용시 주민번호 처리		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 물품이용 대금청구, 기물파손시 손해배상 청구 등을 위해 담보가 필요시, 다른 대체수단(예치금 예치, 신용카드정보 등록 등)으로 목적달성 가능
결론 및 조치사항		주민번호 삭제 및 다른 고유식별정보로 대체

<사례 11> 기업 등의 사옥 출입증 교부시 주민번호 처리		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 생년월일 및 연락처 정보 등으로 대체 가능
결론 및 조치사항		다른 개인정보 항목으로 대체 ※ 다만 주민번호를 수집·이용하지 않고, 단순히 주민번호가 기재된 신분증을 육안으로 확인하고 되돌려 주는 경우는 가능(신분증에 기재된 주민번호 육안 확인은 '주민번호 처리'로 보지 아니함)

<사례 12> 표준약관에 따른 주민번호 처리		
검토	① 법령근거 유무	없음 ⇒「약관의 규제에 관한 법률」에 표준약관 권장 등의 규정은 있으나, 주민번호 처리근거는 없음
	② 불가피성 유무	사안별로 불가피성 유무 다름 ⇒ 법령근거 없는 관행적 주민번호 처리여부 판단 필요
결론 및 조치사항		필요시 해당 법령에 근거 반영

<사례 13> 소송관계 제반 서류에 주민번호 기재		
검토	① 법령근거 유무	없음 ⇒「민사소송규칙」에 따라 법원은 재판업무 수행을 위해 주민번호 처리 가능하나, 법원에 소송을 제기하는 자에 대해서는 주민번호 처리근거 없음
	② 불가피성 유무	있음 ⇒ 소송의 경우 특정인을 명확히 할 필요 존재
결론 및 조치사항		서식 등 법령 반영 필요 (소관 중앙행정기관)

<사례 14> 콜센터(컨택센터) 상담시 주민번호 처리		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 자사 고객 여부 등 단순 본인확인을 위해서는 생년월일, 휴대전화번호 등의 정보 조합으로 대체 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입 ※ 다만 금융회사에서 텔레뱅킹 등을 통해 금융업무를 이용하는 등 '금융거래'에 해당하는 경우에는 주민번호 처리 가능

<사례 15> 정보통신망법에 따른 권리침해신고 접수		
검토	① 법령근거 유무	없음 ⇒ 정보통신망법은 사생활침해·명예훼손 등 권리침해시 침해를 받은 자가 삭제·반박내용 게재 등을 요청할 수 있도록 규정하나(동법 제44조의2) 주민번호 처리에 대해서는 별도 규정 없음
	② 불가피성 유무	없음 ⇒ 대면신고시 신분증 확인, 비대면 신고시 *i*-PIN 등 대체수단 활용 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입

<사례 16> 근로자 퇴직후 주민번호 보관		
검토	① 법령근거 유무	있음 ⇒ 근로자의 경력 증명 등에 관한 정보는 퇴직 후 3년간 별도 보관(근로기준법 제39조, 동법 시행령 제19조)
	② 불가피성 유무	있음 ⇒ 근로자 퇴직 후 재직내역 발급, 근로소득증명 발급, 4대 보험 연계처리 등을 위해 주민번호 처리 필요
결론 및 조치사항		별도 조치 불필요 (현행 주민번호 처리 유지) ※ 단, 근로기준법은 3년간 보관을 규정하고 있으나, 퇴직후 경력증명 요청 등은 3년 이후에도 발생할 수 있으므로 이에 대해서는 소관 중앙행정기관 법령개정 검토 필요

<사례 17> 법령 위임을 통한 협회·단체 등의 교육과정 운영		
검토	① 법령근거 유무	개별 검토 필요 ⇒ 법령의 명문규정 또는 교육과정 지원서식 등에 주민번호 기재항목이 없는 경우 법령근거 없음으로 판단
	② 불가피성 유무	없음 ⇒ 교육이수 증명, 교육경력 발급 등은 다른 개인정보 조합으로 처리 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입

<사례 18> 고속버스 예약시 주민번호 수집		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 신원확인을 위해서는 대체수단 적용이 가능하며, 신용카드 결제 등을 통해서도 신원확인 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입

<사례 19> 사내 주차증, 차량출입증 발급시 주민번호 수집		
검토	① 법령근거 유무	없음
	② 불가피성 유무	없음 ⇒ 신원확인을 위해서는 다른 개인정보 항목 조합으로 가능
결론 및 조치사항		주민번호 삭제 및 필요시 대체수단 도입 ※ 필요시 차량등록증이나 운전면허증 확인 후 반환하거나 주민번호 항목을 삭제하고 사본 접수

붙임 4 주민번호 미수집 전환 시범 사례

1 개 요

○ 사업기간 : ‘13.7 ~ 11월 (4개월) ※ 한국인터넷진흥원 수행

○ 대상 : 학원 등 중소업종 **고객관리프로그램 공급업체 20개**

○ 내용 : 고객관리프로그램 개선 등을 통해 주민번호 미수집 전환

○ 소요비용 : 1개소 당 **평균 190만원** ※ 인건비 기준(투입인력 2명, 4.5일 소요)

○ 사업결과 : 주민번호 미수집 전환 100% 완료

※ 개선 완료된 사례는 ‘프로그램 내려받기’를 통해 각 회원사에 전파

< 주민번호 미수집 전환 시범 실시 현황>

번 호	회 사 명	업종	소재지	주민번호 미수집 전환 방법	비율
1	○○○품	학원	서울	주민번호 일괄삭제	70%
2	○○○소프트	미용실	경기		
3	○○○소프트웨어	스크린골프	경기		
4	(주)코○○○크	유통, 배달	서울		
5	○○○소프트㈜	렌트카	제주		
6	○○○두	복지	서울		
7	(주)○○○케이션즈	출판	서울		
8	주식회사 ○○○컴퍼니	가맹점 관리	서울		
9	○○○ 소프트웨어	도서관	서울		
10	디○○○㈜	스튜디오	부산		
11	○○○소프트뱅크	자동차정비공장	부산		
12	(주)토○○○	병원	서울		
13	○○○소프트	안경	서울		
14	○○○소프트	교회	서울		
15	○○○소프트	PC방	서울	생년월일로 대체	20%
16	○○○온	보험	인천		
17	○○○탑	부동산 중개	경기		
18	○○○소프트	스포츠센터	서울		
19	○○○데이터베이스	애견숍	인천	생년월일, 성별로 대체	5%
20	○○○소프트	차량관리	제주	직원부호로 대체	5%

2 개선 사례

< 주민번호 수집 금지 개선에 소요된 기간 및 비용 >

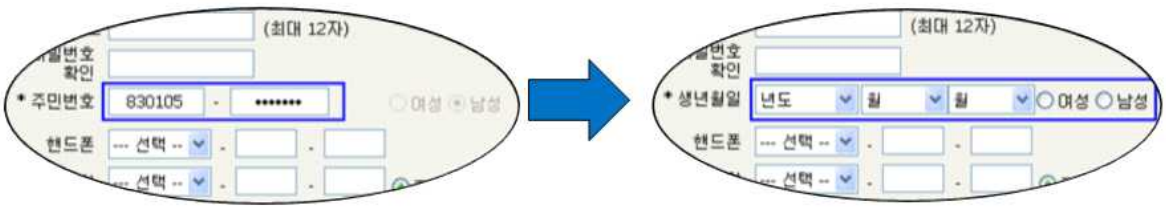
구분	소요기간	투입인력	개발비용
최소	1일	1명	22만원
최대*	25일	4명	2,000만원
평균	4.5일	2명	190만원

* 주민번호 DB가 연계된 타 시스템까지 함께 개선한 경우임

○ (사례 1) PC방 고객관리프로그램 공급업체, 주민번호→생년월일로 대체

업체정보 (○○○소프트)

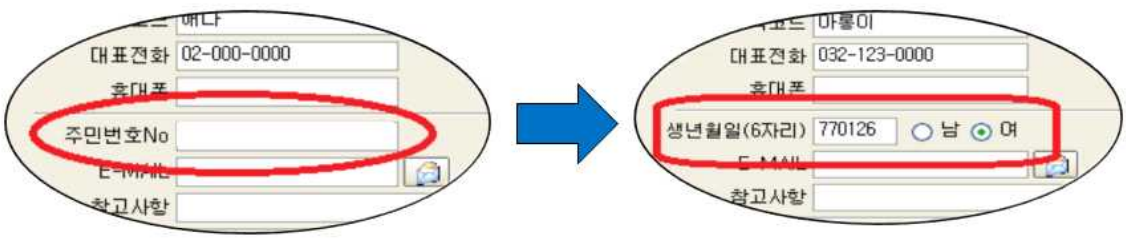
- 업종 : 서울 소재 PC방 고객관리프로그램 공급업체
- 회사규모 : 2,000여개 회원사 보유
- 주민번호 수집 근거 : 없음(관행적으로 수집)
- 개선방법 : 주민번호 → 생년월일로 대체(투입인력 2명, 7일 소요)



○ (사례 2) 애견숍 고객관리프로그램 공급업체, 주민번호→생년월일, 성별로 대체

업체정보 (○○○베이스)

- 업종 : 인천 소재 애견숍 고객관리프로그램 공급업체
- 회사규모 : 10,000여개 회원사 보유
- 주민번호 수집근거 : 없음(관행적으로 수집)
- 개선방법 : 주민번호 → 생년월일, 성별로 대체(투입인력 1명, 2.5일 소요)



○ **(사례 3)** 교회 교인 관리프로그램 공급업체, 주민번호 일괄 삭제

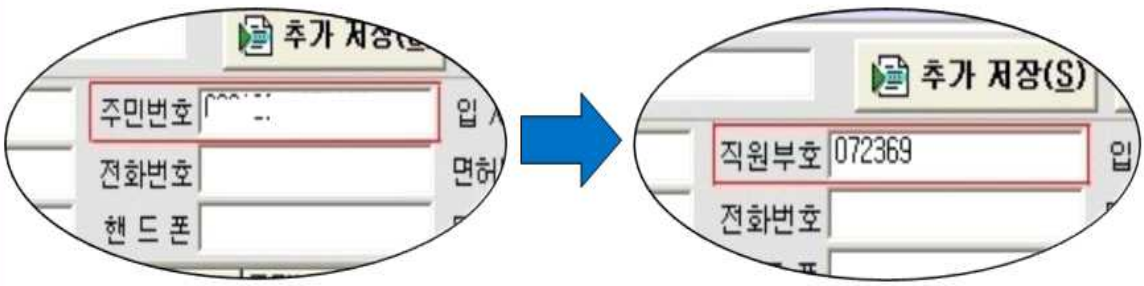
업체정보 (○○소프트)

- 업종 : 서울 소재 교회 교인관리프로그램 공급업체
- 회사규모 : 540여개 회원사 보유
- 주민번호 수집 근거 : 일부 있음(기부금 영수증 발급)
- 개선방법 : 주민번호 일괄 삭제(투입인력 2명, 5일 소요)
  (기부금 영수증 발급시에만 주민번호 입력)

○ **(사례 4)** 차량 관리 프로그램 공급업체, 주민번호→직원부호로 대체

업체정보 (○소프트)

- 업종 : 제주 소재 차량관리 프로그램 공급업체
- 회사규모 : 100여개 회원사 보유
- 주민번호 수집근거 : 없음(관행적으로 수집)
- 개선 방법 : 주민번호 → 직원부호로 대체(투입인력 1명, 3일 소요)



3 개선 방안별 조치사항 예시

1. 주민번호 일괄 삭제시

(1단계) 서비스 분석

▸ DB 구조와 내부에서 활용 중인 주민번호 이용 범위 분석

※ 주민번호가 색인키(Primary Key)로 이용되지 않고 내부에서 별도로 활용하고 있지 않다면 주민번호 일괄 삭제 가능

(2단계) 주민번호 삭제 및 입력창 제거

▸ 테스트 기간을 설정하고, 회원 DB 상에서 주민번호 일괄 삭제 및 고객관리프로그램(또는 웹사이트)에서 주민번호 입력창 제거

※ 개인정보 수집/열람/정정 화면, ID/PW 찾기 화면 등 주민번호 수집을 요구하는 제반 서식 및 업무절차 등 수정

(3단계) 서비스 변경 확인 및 테스트

▸ 주민번호 삭제가 완료된 후 적용 테스트를 통해 서비스 변경 여부, DB 연동 등 각종 기능 이상 유무 등 점검

※ (고려사항) 각종 서비스의 정상 동작 여부, 내부연동 시스템 이상 유무, 기존 DB 백업 및 필요시 복원 가능 여부 등

(4단계) 변경사항 안내

▸ 주민번호를 수집하지 않고, 기 수집한 주민번호는 파기한다는 내용으로 이용약관, 개인정보 처리방침 등을 수정한 후 이용자 안내

※ 서면, 이메일, 문자, 홈페이지 등을 통해 이용자가 알아보기 쉽게 안내

2. 주민번호를 다른 정보로 대체시

(1단계) 서비스 분석

▶ DB 구조와 내부에서 활용 중인 주민번호 이용 범위 분석

※ 주민번호가 색인키(Primary Key)로 이용되거나 내부에서 별도로 활용 중인 경우에는 주민번호를 다른 정보로 대체하는 방향으로 추진

(2단계) 주민번호 대체수단 적용

▶ 현재 주민번호 이용 범위, 내부연동 시스템 구조 등을 고려하여 주민번호를 대체하여 색인키로 활용할 수 있는 정보를 선정

※ 임의 생성정보(회원번호 등), 기존 수집한 정보 또는 그 정보의 조합(전화번호, 성명 등), 기타 다른 정보(*i*-PIN, 공인인증서, 기타 연계정보 등)

▶ 주민번호를 요구하는 각종 업무 절차 수정

※ (예) 주민번호를 이용한 실명확인 → 전화번호 등을 이용한 본인확인
주민번호 확인 후 ID/PW 찾기 → 이메일 인증, 보안질문 등을 이용하고 ID/PW 등을 일부 마스킹하여 제공

(3단계) 서비스 변경 확인 및 테스트

▶ 주민번호 대체가 완료된 후 적용 테스트를 통해 서비스 변경 여부, DB 연동 등 각종 기능 이상 유무 등 점검

※ (고려사항) 각종 서비스의 정상 동작 여부, 내부연동 시스템 이상 유무, 기존 DB 백업 및 필요시 복원 가능 여부 등

(4단계) 변경사항 안내

▶ 주민번호를 수집하지 않고, 기 수집한 주민번호는 파기한다는 내용으로 이용약관, 개인정보 처리방침 등을 수정한 후 이용자 안내

※ 서면, 이메일, 문자, 홈페이지 등을 통해 이용자가 알아보기 쉽게 안내

붙임 5 주민번호 수집 · 이용 허용 법령 사례

o 아래 법령을 포함하여 기존 주민번호 수집 이용을 허용하는 법령은 총 866개

- 법률 77개, 시행령 404개, 시행규칙(서식 포함) 385개

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
금융실명 거래 및 비밀보장에 관한 법률	금융회사 등 (은행, 보험회사 및 카드회사 등)	-금융거래 시 거래자의 성명 · 주민등록번호로 실지명의 확인	<법률> 제3조(금융실명거래) ① 금융회사등은 거래자의 실지명의(이하 "실명"이라 한다)로 금융거래를 하여야 한다. <시행령> 제3조(실지명의) 법 제2조제4호의 규정에 의한 실지명의는 다음 각호의 구분에 따른 명의로 한다. 1. 개인의 경우 주민등록표에 기재된 성명 및 주민등록번호. 다만, 재외국민의 경우에는 여권에 기재된 성명 및 여권번호(여권이 발급되지 아니한 재외국민은 「재외국민등록법」에 의한 등록부에 기재된 성명 및 등록번호)	거래자 (대리인 포함) 주민번호 수집
전자상거래 등에서의 소비자 보호에 관한 법률	전자상거래 사업자 (쇼핑몰 등 전자상거래 업자)	-거래 기록 및 그와 관련한 개인정보(성명 주민번호 등) 보존	<법률> 제6조(거래기록의 보존 등)①사업자는 전자상거래 및 통신판매에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하여야 한다. 이 경우 소비자가 쉽게 거래기록을 열람·보존할 수 있는 방법을 제공하여야 한다. ②제1항의 규정에 의하여 사업자가 보존하여야 할 거래의 기록 및 그와 관련된 개인정보(성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보에 한한다)는 소비자가 개인정보의 이용에 관한 동의를 철회하는 경우에도 정보통신망이용촉진및정보보호등에관한법률 제30조제3항의 규정에 불구하고 이를 보존할 수 있다.	거래가 이루어진 경우에 수집
전자금융 거래법	금융기관 또는 전자금융 업자	-5만 원 이상의 전자화폐를 사용하고자 할 경우 실지명의와 연결하여 관리	<법률> 제16조(전자화폐의 발행과 사용 및 환금) ① 전자화폐를 발행하는 금융회사 또는 전자금융업자(이하 "전자화폐발행자"라 한다)는 전자화폐를 발행할 경우 접근매체에 식별번호를 부여하고 그 식별번호와 「금융실명거래 및 비밀보장에 관한 법률」 제2조제4호에서 규정한 이용자의 실지명의(이하 "실지명의"라 한다) 또는 예금계좌를 연결하여 관리하여야 한다. 다만, 발행권면 최고한도가 대통령령이 정하는 금액 이하인 전자화폐의 경우에는 그러하지 아니하다. <시행령> 제11조(전자화폐의 발행 및 환금방법) ①법 제16조 제1항 단서에서 "대통령령이 정하는 금액"이라 함은 5만원을 말한다.	전자금융 거래 또한 금융실명 거래 의무 적용

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
부가가치세법	재화 또는 용역을 공급하는 자 (일반 사업자)	-재화·용역을 공급받은 자에게 세금계산서를 교부하는 경우, 세금계산서에 공급받은 자의 주소·성명·주민번호 기재	<법률> 제16조(세금계산서) ① 납세의무자로 등록한 사업자가 재화 또는 용역을 공급하는 경우에는 제9조의 시기(대통령령에서 시기를 다르게 정하는 경우에는 그 시기를 말한다)에 다음 각 호의 사항을 적은 계산서(이하 "세금계산서"라 한다)를 대통령령으로 정하는 바에 따라 공급을 받은 자에게 발급하여야 한다. 이 경우 세금계산서를 발급한 후 그 기재사항에 관하여 착오나 정정(訂正) 등 대통령령으로 정하는 사유가 발생한 경우에는 대통령령으로 정하는 바에 따라 세금계산서를 수정하여 발급할 수 있다. 1. 공급하는 사업자의 등록번호와 성명 또는 명칭 2. 공급받는 자의 등록번호 <시행령> 제53조(세금계산서) ②재화 또는 용역을 공급받는 자가 사업자가 아닌 경우에는 법 제16조제1항제2호의 등록번호에 갈음하여 제8조제2항의 규정에 의하여 부여받는 고유번호 또는 공급받는 자의 주소·성명 및 주민등록번호를 기재하여야 한다.	공급받은 자가 사업자가 아닌 경우
소득세법	원천징수 의무자	-기타소득을 지급할 때 원천징수영수증을 발급해야 하며, 영수증에 주민등록번호 기재	<법률> 제145조(기타소득에 대한 원천징수시기와 방법 및 원천징수영수증의 발급① 원천징수의무자가 기타소득을 지급할 때에는 그 기타소득금액에 원천징수세율을 적용하여 계산한 소득세를 원천징수한다. ② 기타소득을 지급하는 원천징수의무자는 이를 지급할 때에 그 기타소득의 금액과 그 밖에 필요한 사항을 적은 기획재정부령으로 정하는 원천징수영수증을 그 소득을 받는 사람에게 발급하여야 한다. 다만, 제21조제1항제15호가목 및 제19호가목·나목에 해당하는 기타소득으로서 대통령령으로 정하는 금액 이하를 지급할 때에는 지급받는 자가 원천징수영수증의 발급을 요구하는 경우 외에는 발급하지 아니할 수 있다. <시행규칙> 제100조(일반서식) 일반서식은 다음 각 호의 어느 하나에 의한다. 25. 법 제133조제1항·제144조제1항·제144조의4·제145조제2항·제156조제12항에 따른 원천징수영수증 및 영 제213조제1항에 규정하는 지급명세서는 별지 제23호서식(1)·별지 제23호서식(2)·별지 제23호서식(3)·별지 제23호서식(4) 또는 별지 제23호서식(5)에 의한다.	시행규칙 서식의 원천징수영수증 기재내용에 주민번호 포함
의료법	병원	- 진단서, 처방전, 진료기록부의 기재사항에 주민번호 포함	<법률> 제17조(진단서 등) ⑤제1항부터 제4항까지의 규정에 따른 진단서, 증명서의 서식·기재사항, 그 밖에 필요한 사항은 보건복지부령으로 정한다.	

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
			제18조(처방전 작성과 교부) ① 의사나 치과의사는 환자에게 의약품을 투여할 필요가 있다고 인정하면 「약사법」에 따라 자신이 직접 의약품을 조제할 수 있는 경우가 아니면 보건복지부령으로 정하는 바에 따라 처방전을 작성하여 환자에게 내주거나 발송(전자처방전만 해당된다)하여야 한다. ②제1항에 따른 처방전의 서식, 기재사항, 보존, 그 밖에 필요한 사항은 보건복지부령으로 정한다. 제22조(진료기록부 등) ① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 갖추어 두고 그 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다. ② 의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자의무기록(電子醫務記錄)을 포함한다. 이하 제40조제2항에서 같다]을 보건복지부령으로 정하는 바에 따라 보존하여야 한다.	
			<시행규칙> 제9조(진단서의 기재 사항) ① 의사·치과의사 또는 한의사가 발급하는 진단서에는 별지 제5호의2서식에 따라 다음 각 호의 사항을 적고 서명날인하여야 한다. 1. 환자의 주소·성명 및 주민등록번호 제12조(처방전의 기재 사항 등) ① 법 제18조에 따라 의사나 치과의사는 환자에게 처방전을 발급하는 경우에는 별지 제9호서식의 처방전에 다음 각 호의 사항을 적은 후 서명(「전자서명법」에 따른 공인전자서명을 포함한다)하거나 도장을 찍어야 한다. 다만, 제3호의 사항은 환자가 요구한 경우에는 적지 아니한다. 1. 환자의 성명 및 주민등록번호 제14조(진료기록부 등의 기재 사항) 법 제22조에 따른 진료기록부·조산기록부와 간호기록부(이하 "진료기록부등"이라 한다)에는 다음 각 호의 구분에 따라 해당 사항을 한글과 한자로 적어야 한다. 다만, 질환명, 검사명, 약제명 등 의학용어는 외국어로 적을 수 있다. 1. 진료기록부 가. 진료를 받은 자의 주소·성명·주민등록번호·병력(病歷) 및 가족력(家族歷) 2. 조산기록부 가. 조산을 받은 자의 주소·성명·주민등록번호	

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
보험업법	금융위원회, 금융감독원, 위 기관의 업무수탁자, 보험요율 산출기관, 보험협회, 보험회사	-각 호에서 정하는 업무 수행에 불가피한 경우	제102조(민감정보 및 고유식별정보의 처리) ① 금융위원회(법 제194조 및 이 영 제100조에 따라 금융위원회의 업무를 위탁받은 자를 포함한다) 또는 금융감독원장(법 제194조 및 이 영 제101조에 따라 금융감독원장의 업무를 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위해 불가피한 경우 「개인정보 보호법 시행령」 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. 1. ~ 16. (생 략) ② 금융위원회(법 제194조 및 이 영 제100조에 따라 금융위원회의 업무를 위탁받은 자를 포함한다) 또는 금융감독원장(법 제194조 및 이 영 제101조에 따라 금융감독원장의 업무를 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위해 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. 1. ~ 11. (생 략) ③ 보험요율 산출기관은 법 제176조제3항제1호·제2호 및 이 영 제86조제2호에 따른 사무를 수행하기 위하여 불가피한 경우 제2항 각 호 외의 부분에 따른 개인정보가 포함된 자료를 처리할 수 있다. ④ 보험협회의 장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. 1. ~ 4. (생략) ⑤ 보험회사는 다음 각 호의 사무를 수행하기 위하여 필요한 범위로 한정하여 해당 각 호의 구분에 따라 「개인정보 보호법」 제23조에 따른 민감정보 중 건강에 관한 정보(이하 이 항에서 "건강정보"라 한다)나 같은 법 시행령 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호(이하 이 항에서 "고유식별정보"라 한다)가 포함된 자료를 처리할 수 있다.	
자격기본법	공인자격 관리자	-공인자격증 기재사항 및 관리를 위해 주민번호 수집・이용 가능	<법률> 제23조(공인자격의 취득 등) ⑤공인자격증의 기재사항 등에 관하여 필요한 사항은 교육부령으로 정한다. <시행규칙> 제6조(공인자격증의 기재 사항) 법 제23조제5항에 따른 공인자격증에는 다음 각 호의 사항이 포함되어야 한다.	

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
			3. 자격취득자의 성명 및 주민등록번호 제32조(자격에 관한 정보의 내용 등) ① 법 제34조제1항에 따라 국가자격관리자와 공인자격관리자는 다음 각 호의 사항에 대한 정보를 체계적으로 관리하여야 한다. 1. 성명·주민등록번호 등 자격취득자의 인적사항	
고용보험법	사업주 또는 훈련기관	-직업능력개발 훈련비용 청구를 위한 지원서 작성시 훈련생의 주민번호 기재	<법률> 제41조(사업주에 대한 직업능력개발 훈련비용의 지원) ④ 직업능력개발 훈련의 훈련비와 훈련수당의 지원범위, 지원상한액 및 지원신청절차와 그 밖에 지원에 필요한 사항은 고용노동부령으로 정한다. <시행규칙> 제60조(사업주에 대한 직업능력개발 훈련비용의 지원신청) ② 제1항에 따른 직업능력개발 훈련의 훈련비, 훈련수당 및 임금의 일부에 해당하는 금액에 대하여 지원을 받으려는 자는 별지 제58호서식의 사업주 직업능력개발 훈련비용 지원 신청서를 훈련이 끝난 후나 매 3개월간의 훈련실시 후 30일 이내에 그 사업장의 소재지를 관할하는 공단 분사무소에 제출하여야 한다. 다만, 사업주가 고용노동부장관이 정하는 결제시스템을 이용하여 훈련비를 훈련기관에 지급한 경우에는 사업주는 그 훈련기관에게 별지 제58호의2서식의 사업주 직업능력개발 훈련비용 지원 신청서(훈련기관용)에 따라 직업능력개발 훈련비용의 지원신청을 대행하게 할 수 있다.	시행규칙 별지 서식에 주민번호 기재
전기통신사업법	전기통신사업자 → 수사기관	-수사기관이 전기통신사업법에 의한 통신자료 요청 시 주민등록번호 제출	<법률> 제83조(통신비밀의 보호) ③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범 처벌법」 제10조제1항·제3항·제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 “통신자료제공”이라 한다)을 요청하면 그 요청에 따를 수 있다. 2. 이용자의 주민등록번호	
전자서명법	공인인증기관	-공인인증서 발급 시 발급자의 성명・주민등록번호 등으로 신원확인	<법률> 제15조(공인인증서의 발급) ① 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다. 이 경우 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다. <시행규칙> 제13조의2(신원확인의 기준 및 방법) ① 공인인증기관은 법 제15조제1항 후단의 규정에 의하여 공인	

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
			인증서를 발급받고자 하는 자의 신원을 확인하는 경우에는 다음 각호의 구분에 따른 실지명의를 기준으로 하여야 한다. 1. 개인의 경우 가. 주민등록표에 기재된 성명 및 주민등록번호. 다만, 재외국민의 경우에는 여권에 기재된 성명 및 여권번호(여권이 발급되지 아니한 재외국민의 경우에는 「재외국민등록법」에 의한 등록부에 기재된 성명 및 등록번호)	
방송법	방송사업자	-방송사업자에 대해 정보 공개 요구시 제출자료	<시행령> 제65조(정보의 공개) ① 법 제90조제5항의 규정에 의하여 종합편성 또는 보도전문편성을 행하는 방송사업자(「공공기관의 정보공개에 관한 법률」의 적용을 받는 방송사업자를 제외하며, 이하 이 조에서 "종합·보도방송사업자"라 한다)에 대하여 정보의 공개를 요구하는 자는 다음 각호의 사항을 기재한 정보공개신청서를 방송사업자에게 제출하여야 한다. 1. 청구인의 성명·주민등록번호 및 주소	
벤처기업 육성에 관한 특별조치법	벤처기업	-주식교환시 주주의 주민번호 기재사항	<법률> 제15조(벤처기업의 주식교환) ③ 제1항에 따라 주식교환을 하려는 벤처기업은 다음 각 호의 사항이 포함된 주식교환계약서를 작성하여 주주총회의 승인을 받아야 한다. 이 경우 주주총회의 승인 결의에 관하여는 「상법」 제434조를 준용한다. 5. 다른 주식회사의 주요주주와 주식을 교환할 경우 주주의 성명, 주민등록번호, 교환할 주식의 종류 및 수량 제15조의4(신주발행에 의한 주식 교환 등) ② 제1항에 따른 주식교환을 하려는 벤처기업은 다음 각 호의 사항이 포함된 주식교환계약서를 작성하여 주주총회의 승인을 받아야 한다. 이 경우 주주총회의 승인 결의에 관하여는 「상법」 제434조를 준용한다. 4. 다른 주식회사의 주요주주와 주식을 교환할 경우 주주의 성명, 주민등록번호, 교환할 주식의 종류 및 수량	

붙임 6 주민번호 수집 금지 정책 관련 Q&A

Q1 왜 주민번호를 수집·이용하지 않아야 하나요?

- 주민번호는 본래 행정목적으로 국가나 지방자치단체가 국민을 특정하기 위해 도입되었으나, 사회 전 분야에 걸쳐 과도하게 수집·이용되고 있어 유출 등으로 인한 피해 우려와 불안감이 늘고 있습니다.
- 개인정보 유출로 인한 피해 및 분쟁 방지를 위해서는 근본적으로 주민번호의 수집·이용을 최소화하여 주민번호 미수집 환경을 조성하는 것이 바람직합니다.

Q2 '14년8월부터 주민번호 수집이 전면 금지된다는데 앞으로 어떻게 준비해야 하는지 ?

- 주민번호는 유일성, 평생불변성 등의 특징으로 인하여 한번 유출시에도 지속적인 피해가 발생할 수 있는 중요한 정보입니다. 이에 정부에서는 불필요한 주민번호 수집 관행을 근절하고 유출 및 오남용으로 인한 피해를 예방하고자, 지난 2013년 8월 6일 주민번호 수집 금지 등을 주요 내용으로 개인정보보호법을 개정 공포하였습니다.
- 따라서, 공공기관 및 민간사업자 등은 개정 개인정보보호법이 시행되는 2014년 8월 7일 전까지 소관업무 수행과 관련한 주민번호 수집 및 이용 실태를 스스로 점검하여 불필요한 경우에는 주민번호를 수집하지 않도록 하거나 생년월일, I-pin, 휴대폰번호, 회원번호 등으로 대체하여야 하며, 소관업무의 성격상 주민번호 수집이 불가피한 경우에는 해당 업무와 관련한 정부 부처에 법령 근거 마련을 요청하여야 합니다. 아울러, 법령 근거가 없는 경우에는 기존에 수집하여 보관 중인 주민번호를 2016년 8월 6일 이전까지 모두 파기하여야 합니다.
- 현재, 안전행정부는 개정 개인정보보호법 시행에 대비하여 한국인터넷진흥원을 통해 주민번호 미수집 관련 상담 및 컨설팅을 지원하고 있으니 필요한 경우 궁금한 사항이나 세부 조치 등 필요사항에 대하여 문의하시기 바랍니다.

<주민번호 전환 지원 전담반(한국인터넷진흥원)>

◇ 대표 문의처 : 국번 없이 118번

◇ 관련 법제도 상담 및 컨설팅 문의

☞ 이메일 : jumin@kisa.or.kr

◇ 대체수단 도입 등 기술지원 상담 및 컨설팅 문의

☞ 이메일 : privacy_support@kisa.or.kr

Q3 회사내 직원들의 주민번호를 수집할 수 있는지 ?

- 개정 개인정보보호법 제24조의2제1항제1호에 따라 개인정보처리자는 법령에서 구체적으로 주민번호의 처리를 요구 허용하는 경우에는 주민번호를 수집하여 이용할 수 있으며, 사업주는 소속 근로자의 국민연금, 고용보험, 건강보험, 산재보험 등 4대 보험 가입과 세금 원천징수 등을 위해 관련 법령에서 정하는 바에 따라 해당 근로자의 주민번호를 수집하여야 합니다.
- 따라서, 사업주는 개정 개인정보보호법이 시행된 이후에도 자신의 비용으로 임금을 지급하고 있는 소속 직원의 주민번호를 수집하여 인사관리나 급여 지급 등의 목적으로 이용할 수 있습니다.

Q4 웹사이트 회원 가입 신청자가 본인이 맞는지 여부를 확인하기 위하여 주민번호를 이용한 실명확인을 할 수 있나요 ?

- 웹사이트 회원가입 신청자가 본인이 맞는지 여부를 확인하기 위한 방법으로는 주민번호를 이용한 실명확인 이외에도 휴대전화번호, 공인인증서, 아이핀(*i*-PIN) 등 다양한 본인확인 방법이 있으므로 주민번호를 반드시 수집하여야 할 필요는 없습니다.
- 따라서, 법령상 구체적 근거가 없다면 주민번호를 이용한 실명확인 방법 보다는 휴대전화번호 등 대체수단을 이용한 본인확인 방법을 사용하시기 바랍니다.

Q5 멤버십 회원 포인트 부여 및 사용을 위해 주민번호를 수집·이용해도 괜찮은가요?

- 멤버쉽 회원의 포인트 관리를 위해 해당 회원의 주민번호를 수집하여 포인트 이용실적 합산 등을 위해 이용하는 경우는 그 목적의 적합성이나 대체수단 적용 가능성 등을 고려할 때 개정 개인정보보호법에 따라 주민번호 수집을 허용하는 경우로 보기는 어렵습니다.(법령에서 구체적으로 요구 허용하는 경우, 급박한 생명·신체·재산상 이익을 위해 필요한 경우 등에 한하여 주민번호 처리가 허용됨)
- 따라서, 이러한 경우에는 주민번호를 휴대폰번호, 회원번호, *i*-PIN, 생년월일 등으로 대체하고 기존에 수집하여 보관중인 주민번호는 개정 개인정보보호법 시행 후 2년(2016.8.6일까지) 이내에 모두 삭제하여야 합니다.

Q6 민간회사 건물 출입시 외부방문자의 주민번호를 기록 보관할 수 있나요 ?

- 민간회사 건물에서 외부 방문자의 성명, 연락처, 방문목적 등의 정보를 수집하는 것은 해당 건물 또는 사무실의 보안 유지나 시설물 보호 등을 위해 일정 부분 필요하다고 볼 수 있으나, 주민번호와 같은 중요한 정보까지 수집하여야 할 불가피성이 있다고 보기는 어렵습니다.
- 따라서, 이러한 경우에는 해당 건물에 출입하는 외부 방문자의 출입 목적과 필요시 연락을 취할 수 있는 전화번호 등 필요 최소한의 개인정보에 한하여 수집토록 하고, 주민번호는 수집하지 않도록 해야 할 것입니다.

Q7 콜센터 상담시 고객 본인 확인을 위해 주민번호 수집이 가능한가요 ?

- 일반적으로 콜센터 상담시에는 해당 통화 상대방이 고객 본인인지 여부를 확인하기 위하여 해당 고객과의 거래 과정에서 수집한 각종 개인정보를 물어볼 수 있으나, 생년월일, 휴대전화번호 등의 다양한 정보를 이용하여 고객 본인 여부를 충분히 확인할 수 있으므로 반드시 주민번호를 요구하여야 할 필요성이 낮고 법적 근거 또한 없는 경우로 볼 수 있습니다.
- 따라서, 콜센터가 고객 본인 확인을 위하여 필요한 경우에는 생년월일, 휴대전화번호, 기타 거래내역 등의 정보를 이용하여야 할 것이며 주민번호와 같은 중요한 정보를 요구하여서는 아니 될 것입니다.
- 다만, “금융실명 거래 및 비밀보장에 관한 법률” 등에 따라 은행 등 금융회사는 거래자의 실지명의(개인의 경우 성명 및 주민번호)로 금융거래를 하여야 할 법적 의무를 가지므로, 금융회사 콜센터가 금융거래를 위한 경우에는 해당 고객의 실지명의 확인을 위해 주민번호를 요구할 수 있습니다.

Q8 채용시험 대상자의 주민번호 수집이 가능한가요 ?

- 주민번호 유출이나 오남용 피해 우려 등을 고려할 때 입사지원 서류 제출이나 채용시험 응시 등 입사지원 단계에 있는 구직자의 경우에는 아직 근로계약 체결 여부가 확정되지 않은 상태이므로 사용자가 구직자의 주민번호를 수집하여야 하는 필요성이나 법적 근거가 있다고 볼 수 없습니다.
- 따라서, 아직 입사지원 단계에 있는 구직자의 경우에는 주민번호 대신 생년월일이나 휴대폰번호 등을 수집하는 것으로 대체하고, 향후 채용 여부가 확정된 후 사용자와 근로계약을 체결하는 단계에서는 고용보험 등 4대 보험 가입, 급여 원천징수 등을 위해 관련 법령에서 정하는 바에 따라 사용자가 해당 최종 합격자의 주민번호를 수집하여야 할 것입니다.

Q9 주민번호 앞자리(생년월일)는 사용 가능한가요?

- 주민번호 앞자리의 생년월일은 주민번호의 체계에 따라 생성되는 것이 아니라, 출생신고 시 국민이 공공기관에 신고한 날짜를 토대로 정의되는 숫자 열입니다.
- 따라서, 생년월일은 주민번호를 이용한 숫자열이라 보기 어려우며, 이용자의 동의를 받아 수집·이용이 가능합니다.

Q10 주민번호 뒷자리만 사용하는 것은 괜찮은가요?

- 주민번호의 뒷자리를 수집·이용하여 회원의 유일성과 식별성을 확보하는 것은 주민번호의 체계를 활용하여 주민번호의 고유한 특성을 이용하는 것이므로 주민번호를 수집·이용하는 경우에 해당한다고 볼 수 있습니다.
- 따라서, 법령상 주민번호를 수집할 수 있는 구체적 근거가 없다면 주민번호의 뒷자리를 수집·이용할 수 없습니다.

Q11 14세 미만 아동의 회원가입 시 법정대리인 동의 여부에 대한 증명을 위해 주민번호를 수집하고 있는데, 어떻게 해야 하나요?

- 「개인정보보호법」 제22조에서 만14세 미만 아동의 개인정보를 수집·이용하는 경우에는 반드시 법정대리인의 동의를 받도록 명시하고 있습니다.
- 하지만 법정대리인의 동의 여부에 대한 증명을 위해 주민번호를 수집·이용하는 것은 법령상 특별한 근거가 없으며, 휴대전화번호, 아이핀 등 다른 대체수단을 이용하여 해당 조항의 목적 달성이 가능하므로 굳이 주민번호를 수집하지 않는 것이 바람직할 것입니다.

Q12 현금영수증 발급을 위해 주민번호를 이용하고 있는데 어떻게 해야 하나요?

- 「조세특례제한법」에 따라서 현금영수증 사업자는 현금영수증 결제를 승인하고 전송할 수 있어 주민번호 수집·이용이 가능합니다.
- 그러나 현금영수증 사업자가 아닌 경우 현금영수증 발행을 위한 주민번호의 수집·이용에 대한 법률근거가 없기 때문에 주민번호의 사용이 금지되며 현금영수증 발행업체에서 직접 제공하는 입력창을 통해서만 이용자의 정보를 제공받을 수 있습니다.

Q13 법령에서 주민번호 수집·이용을 허용하는 경우란 어떠한 경우 인가요?

- 법령(법률, 시행령, 시행규칙)상 주민번호 수집을 요구하거나 허용하는 내용이 구체적으로 명시된 경우를 말합니다. 예를 들면, 금융실명거래법에서는 금융회사의 거래 시 주민번호를 통해 이용자의 실지명의를 확인해야 함을 명시하고 있으므로 금융회사가 금융거래와 관련하여 거래자의 실지명의 확인을 위한 경우에는 주민번호 사용이 가능합니다.

Q14 고객관리를 위해서 사용하던 주민번호를 삭제하고 싶습니다, 어떻게 해야 하나요?

- DB 등을 이용해 고객정보를 관리하고 계신다면 해당 DB 테이블을 검토하여 주민번호를 일괄 삭제하거나 주민번호를 다른 정보로 대체한 후 문제가 없다면 주민번호를 삭제하시면 됩니다.
- 별도의 고객관리프로그램 등을 통해 관리하고 계신다면 먼저 해당 프로그램의 제작사에 프로그램 업데이트 등 수정사항이 있는지 문의하시기 바랍니다.

Q15 기존에 수집했던 주민번호는 어떻게 해야 하나요?

- 주민번호를 수집하지 않기로 결정하셨다면, 기존에 수집했던 주민번호는 외부로 유출되지 않도록 주의하여 파기하시기 바랍니다. 문서 형태로 된 경우에는 파쇄 등의 방법, 전자적 파일 형태인 경우에는 복원할 수 없도록 적절한 삭제 방법을 취하시기 바랍니다.

Q16 주민번호를 수집하지 않으면 어떻게 사용자를 식별할 수 있나요?

- 기존의 주민번호를 대체하는 수단인 아이핀, 공인인증서, 휴대폰 인증 등을 사용하실 수 있습니다. 아울러 아이핀을 도입하실 경우 사용자를 식별할 수 있는 DI(중복가입확인정보), CI(연계정보) 등을 제공받을 수 있습니다.
- 독립적인 고객관리프로그램 등을 이용하시는 경우에는 주민번호 대신 이름, 전화번호의 조합과 같이 기존에 수집된 다른 정보들을 활용하는 경우에도 사용자 식별이 가능할 것으로 보입니다.

Q17 주민번호를 사용하지 않으면 아이디나 비밀번호를 분실한 사용자에게 어떻게 안내해야 하나요?

- 대체수단을 이용해 사용자를 확인하거나, 이용자 본인만 알 수 있는 질문과 답변을 통해 새로운 비밀번호를 설정하는 등 여러 가지 수단이 있을 수 있습니다.

Q18 주민번호를 사용하지 않으려면 꼭 대체수단을 도입해야 하나요?

- 필요한 경우 대체수단을 도입하는 것을 권장하는 것이며, 반드시 대체수단을 도입해야만 하는 것은 아닙니다.
- 만약, 이용자의 신원확인이나 중복가입확인 등이 필요하지 않은 경우라면 이메일을 통해 인증메일을 보내거나 휴대폰을 통해 인증코드를 발송하는 등의 방법으로 실사용자 여부를 확인할 수 있습니다.

Q19 연령확인을 위해 주민번호를 사용하고 있습니다. 주민번호 외에 연령확인, 성인인증 등을 할 수 있는 방법이 있나요?

- 법령상 연령확인, 성인인증 등이 필요하지만 주민번호를 사용할 근거가 없는 경우에는 대체수단을 통해 해결할 수 있습니다.
- 예를 들어 아이핀을 도입하신 경우, 인증결과로 연령대 정보, 성별 정보 등을 받을 수 있으므로 이를 이용하시면 될 것으로 보입니다.

Q20 주민번호를 이용하지 않는 본인확인 수단에는 어떤 것들이 있나요?

- 현재 주민번호를 대신하여 본인확인을 할 수 있는 수단에는 아이핀, 공인인증서, 휴대폰 인증 등의 방법이 있습니다.

Q21 아이핀에 대해 자세히 알고 싶습니다.

- 아이핀은 주민번호를 사용하지 않고 본인확인을 할 수 있는 수단입니다. 이용자는 복잡한 인증 절차를 거치지 않고 아이디, 비밀번호를 통해 본인확인을 받을 수 있고, 사업자는 이용자의 주민번호를 수집 및 저장하지 않으므로 주민번호의 유출을 근본적으로 예방할 수 있습니다.

Q22 아이핀을 도입하고 싶은데, 어디에 문의해야 하나요?

- 아이핀은 민간 본인확인기관에서 도입·발급·운영하는 민간 아이핀과 안전행정부의 공공아이핀센터에서 도입·발급·운영하는 공공아이핀으로 구분됩니다.
- 따라서, 사업자는 업종 특성을 고려하여 선택하고 본인확인기관에 문의하여 아이핀 도입에 대한 도움을 받을 수 있습니다.

※ 민간아이핀 : NICE아이핀(1588-2486), SIREN24 (1577-1006)

※ 공공아이핀 : 공공아이핀센터(02-818-3050)

Q23 공인인증서는 무엇인가요?

- 공인인증서는 온라인상 금융거래 시 신원확인, 문서의 위·변조, 거래 사실의 부인 방지 등을 목적으로 전자서명법 제15조에 따라 공인인증기관이 발행하는 전자적 문서입니다.
- 따라서, 사업자가 본인확인을 수행할 때, 이용자는 공인인증서를 제시하고 비밀번호 및 개인정보를 함께 제공하여 본인임을 확인받을 수 있습니다.

Q24 휴대폰 인증은 무엇이며, 어떻게 도입하나요?

- 휴대폰 인증은 이용자가 휴대전화 번호와 간단한 인적사항을 기입한 후, 휴대폰 인증 서비스 업체에서 발송하는 SMS 인증번호 확인을 통해 인증을 수행하는 방식입니다.
- 휴대폰 인증의 도입 방법 및 절차는 사업자의 업종 및 규모에 따라 달라질 수 있으므로 휴대폰 인증을 제공하는 본인확인기관에 연락하여 자세한 정보 및 해당 시스템 도입에 따른 사항을 상담 받을 수 있습니다.

개인정보 비식별 조치 가이드라인

-비식별 조치 기준 및 지원·관리체계 안내-

국민을 즐겁게

국무조정실 행정자치부 방송통신위원회
금융위원회 미래창조과학부 보건복지부

빅데이터, IoT(사물인터넷) 등 새로운 IT 기술과 융합산업의 출현은 세계 최고 수준의 IT강국으로 자리매김한 우리나라에게 또 다른 도약의 기회가 되고 있으나, 한편으로 그러한 기술 활용과정에서 발생할 수 있는 개인정보 침해 우려는 신산업 발전과 개인정보의 보호를 동시에 조화롭게 모색해야 하는 과제를 제기하고 있습니다.

이에 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부 등 관계부처가 합동으로 현행 개인정보 보호 법령의 틀 내에서 빅데이터가 안전하게 활용될 수 있도록 하는데 필요한 개인정보의 비식별 조치 기준과 비식별 정보의 활용 범위 등을 명확히 제시함으로써 기업의 불확실성을 제거하여 기업투자와 산업 발전을 도모하는 한편, 국민의 개인정보인권 보호에도 소홀함이 없도록 하고자 합니다.

아울러, 이 가이드라인에 따라 정보주체를 알아볼 수 없도록 비식별 조치를 적정하게 한 비식별 정보는 개인정보가 아닌 것으로 추정되며, 따라서 빅데이터 분석 등에 활용이 가능합니다.

다만, 비식별 정보도 기술발전, 데이터 증가 등에 따른 재식별 가능성이 있음을 고려하여 재식별 방지를 위한 관리적 · 기술적 안전조치 등을 통해 안전하게 활용되고 관리되어야 함을 알려드립니다.

2016. 6. 30. 관계부처 합동

Contents

Ⅰ 추진 배경 2

Ⅱ 비식별 조치 기준 3
1. 조치 개요 3
2. 단계별 조치 기준 4

Ⅲ 지원 및 관리체계 17
1. 개인정보 비식별 조치 지원 17
2. 전문기관을 통한 기업 간 정보집합물 결합 지원 18
3. 재식별 시 법적 제재 21

참고
참고 1 ● 비식별 정보의 산업적 활용(예시) 24
참고 2 ● 국내외 동향 26
참고 3 ● 개인정보 비식별 조치 방법 30
참고 4 ● 비식별 조치 적정성 평가단 세부 평가수행 방법 42

부록
부록 1 ● 개인정보 보호 관련 법령 통합 해설서 51
부록 2 ● 질의 및 응답(Q&A) 61

개인정보 비식별 조치 가이드라인

– 비식별 조치 기준 및 지원 · 관리체계 안내 –

Ⅰ 추진 배경

Ⅱ 비식별 조치 기준

Ⅲ 지원 및 관리체계

I 추진 배경

- 빅데이터, IoT 등 IT 융합기술 발전으로 데이터 이용 수요가 급증함에 따라 미국 · 영국 등 주요 선진국은 데이터 산업 활성화를 위한 정책 추진 중
- 이에 빅데이터 활용에 필요한 비식별 조치 기준 · 절차 · 방법 등을 구체적으로 안내하여 안전한 빅데이터 활용기반 마련과 개인정보 보호 강화를 도모

1 정부 3.0 및 빅데이터 활용 확산에 따른 데이터 활용가치 증대

- 공공정보 개방 · 공유는 투명하고 효율적인 정부 운영에, 빅데이터 활용은 과학적 정책 집행 및 맞춤형 서비스 제공에 필수적인 수단
- 특히, 빅데이터 분석, IoT 기술 등을 통한 새로운 서비스 창출과 신산업 활성화에 데이터의 활용가치 증대

2 개인정보 보호 강화에 대한 사회적 요구 지속

- 크고 작은 개인정보 유출 사고가 지속되어 개인정보 보호 정책을 강화해야 한다는 사회적 요구가 계속
- 다양한 데이터 활용을 필요로 하는 새로운 산업과 기술 발전으로 개인정보 침해 위험도 증가 추세

3 '보호와 활용'을 동시에 모색하는 세계적 정책변화에 적극 대응

- 미국 · 영국 등 주요 선진국은 개인정보 침해가능성을 최소화하면서 데이터 산업 활성화를 위한 정책 추진 중
- 사생활 침해 방지를 위한 안전장치 마련과 동시에 비식별 조치된 정보는 산업적으로 활용할 수 있도록 구체적인 가이드 제시 필요

Ⅱ 비식별 조치 기준

1 조치 개요

- 본 가이드라인은 개인정보를 비식별 조치하여 이용 또는 제공하려는 사업자 등이 준수하여야 할 조치 기준을 제시한 것임

  ※ 통계법 등 관련법령에 따라 개인정보를 수집 · 이용하는 경우에는 당해 법령에 따라 처리

- 단계별 조치사항

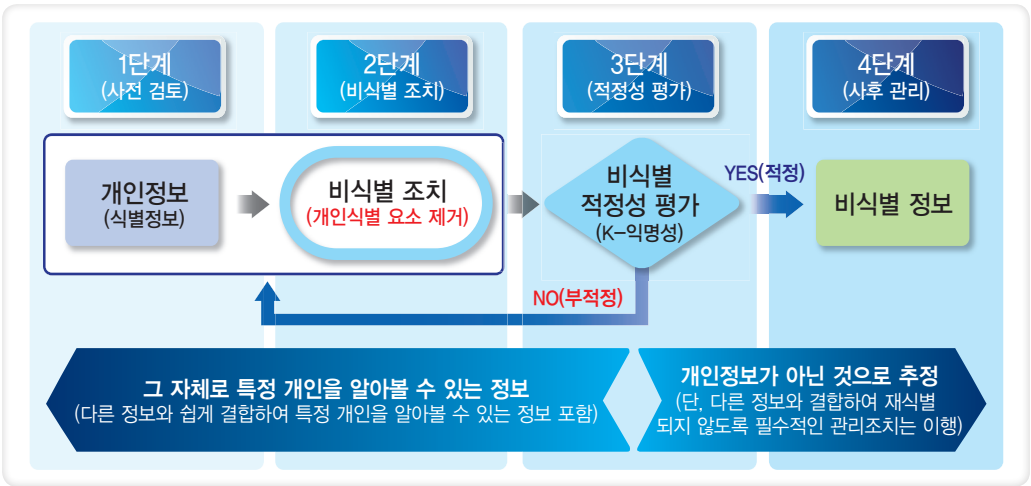
  ① **(사전 검토)** 개인정보에 해당하는지 여부를 검토 후, 개인정보가 아닌 것이 명백한 경우 법적 규제 없이 자유롭게 활용(4쪽 참조)

  ② **(비식별 조치)** 정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용, 개인을 알아볼 수 없도록 하는 조치(5~8쪽 참조)

  ③ **(적정성 평가)** 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는지를 「비식별 조치 적정성 평가단」을 통해 평가(9~13쪽 참조)

  ④ **(사후관리)** 비식별 정보 안전조치, 재식별 가능성 모니터링 등 비식별 정보 활용 과정에서 재식별 방지를 위해 필요한 조치 수행(14~16쪽 참조)

● 비식별 조치 및 사후관리 절차 ●



2 단계별 조치 기준

2-① 사전 검토 단계 : 개인정보 해당 여부 검토

- 빅데이터 분석 등을 위해 정보를 처리하려는 사업자 등은 해당 정보가 개인정보인지 여부에 대해 아래 기준을 참조하여 판단

- 해당 정보가 개인정보에 해당하지 않는 것이 명백한 경우에는 별도 조치 없이 빅데이터 분석 등에 활용 가능

  ⇨ 개인정보에 해당한다고 판단되는 경우 다음 단계의 조치 필요

〈 참고 〉 개인정보 해당 여부 판단 기준

가. 개인정보 보호법 등 관련 법률에서 규정하고 있는 개인정보의 개념은 다음과 같으며, 이에 해당하지 않는 경우에는 개인정보가 아님

나. 개인정보는 ⅰ)살아 있는 ⅱ)개인에 관한 ⅲ)정보로서 ⅳ)개인을 알아수 있는 정보이며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 ⅴ)다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 포함

ⅰ) (살아있는) 자에 관한 정보이어야 하므로 사망한 자, 자연인이 아닌 법인, 단체 또는 사물 등에 관한 정보는 개인정보에 해당하지 않음

ⅱ) (개인에 관한) 정보이어야 하므로 여럿이 모여서 이룬 집단의 통계값 등은 개인정보에 해당하지 않음

ⅲ) (정보)의 종류, 형태, 성격, 형식 등에 관하여는 특별한 제한이 없음

ⅳ) (개인을 알아볼 수 있는 정보)이므로 특정 개인을 알아보기 어려운 정보는 개인정보가 아님

- 여기서 '알아볼 수 있는'의 주체는 해당 정보를 처리하는 자(정보의 제공 관계에 있어서는 제공받은 자를 포함)이며, 정보를 처리하는 자의 입장에서 개인을 알아볼 수 없다면 그 정보는 개인정보에 해당하지 않음

ⅴ) (다른 정보와 쉽게 결합하여)란 결합 대상이 될 다른 정보의 입수 가능성이 있어야 하고, 또 다른 정보와의 결합 가능성이 높아야 함을 의미

- 즉, 합법적으로 정보를 수집할 수 없거나 결합을 위해 불합리한 정도의 시간, 비용 등이 필요한 경우라면 "쉽게 결합"할 수 있는 상태라고 볼 수 없음

※ 자세한 내용은 부록 「개인정보 보호 관련 법령 통합해설서」 참조

2-② 비식별 조치 단계 : 비식별 조치기법 적용

식별자(Identifier) 조치 기준

- 정보집합물에 포함된 식별자*는 원칙적으로 삭제 조치

  * '식별자'란 개인 또는 개인과 관련한 사물에 고유하게 부여된 값 또는 이름

- 다만, 데이터 이용 목적상 반드시 필요한 식별자는 비식별 조치 후 활용

〈 예시 〉 식별자

- 고유식별정보(주민등록번호, 여권번호, 외국인등록번호, 운전면허번호)
- 성명(한자 · 영문 성명, 필명 등 포함)
- 상세 주소(구 단위 미만까지 포함된 주소)
- 날짜정보 : 생일(양/음력), 기념일(결혼, 돌, 환갑 등), 자격증 취득일 등
- 전화번호(휴대전화번호, 집전화, 회사전화, 팩스번호)
- 의료기록번호, 건강보험번호, 복지 수급자 번호
- 통장계좌번호, 신용카드번호
- 각종 자격증 및 면허 번호
- 자동차 번호, 각종 기기의 등록번호 & 일련번호
- 사진(정지사진, 동영상, CCTV 영상 등)
- 신체 식별정보(지문, 음성, 홍채 등)
- 이메일 주소, IP 주소, Mac 주소, 홈페이지 URL 등
- 식별코드(아이디, 사원번호, 고객번호 등)
- 기타 유일 식별번호 : 군번, 개인사업자의 사업자 등록번호 등

※ 美 「HIPAA 프라이버시 규칙」을 참고하여 작성

속성자(Attribute value) 조치 기준

- 정보집합물에 포함된 속성자*도 데이터 이용 목적과 관련이 없는 경우에는 원칙적으로 삭제

  * '속성자'란 개인과 관련된 정보로서 다른 정보와 쉽게 결합하는 경우 특정 개인을 알아볼 수도 있는 정보

  – 데이터 이용 목적과 관련이 있는 속성자 중 식별요소가 있는 경우에는 가명처리, 총계처리 등의 기법을 활용하여 비식별 조치

- 희귀병명, 희귀경력 등의 속성자는 구체적인 상황에 따라 개인 식별 가능성이 매우 높으므로 엄격한 비식별 조치 필요

〈 예시 〉 속성자	
개인 특성	• 성별, 연령(나이), 국적, 고향, 시 · 군 · 구명, 우편번호 병역여부, 결혼여부, 종교, 취미, 동호회 · 클럽 등 • 흡연여부, 음주여부, 채식여부, 관심사항 등
신체 특성	• 혈액형, 신장, 몸무게, 허리둘레, 혈압, 눈동자 색깔 등 • 신체검사 결과, 장애유형, 장애등급 등 • 병명, 상병(傷病)코드, 투약코드, 진료내역 등
신용 특성	• 세금 납부액, 신용등급, 기부금 등 • 건강보험료 납부액, 소득분위, 의료 급여자 등
경력 특성	• 학교명, 학과명, 학년, 성적, 학력 등 • 경력, 직업, 직종, 직장명, 부서명, 직급, 전직장명 등
전자적 특성	• 쿠키정보, 접속일시, 방문일시, 서비스 이용 기록, 접속로그 등 • 인터넷 접속기록, 휴대전화 사용기록, GPS 데이터 등
가족 특성	• 배우자 · 자녀 · 부모 · 형제 등 가족 정보, 법정대리인 정보 등

비식별 조치 방법

- 가명처리, 총계처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹 등 여러 가지 기법을 단독 또는 복합적으로 활용

  ※ '가명처리' 기법만 단독 활용된 경우는 충분한 비식별 조치로 보기 어려움

- 각각의 기법에는 이를 구현할 수 있는 다양한 세부기술이 있으며, 데이터 이용 목적과 기법별 장 · 단점 등을 고려하여 적절한 기법 · 세부기술을 선택 · 활용

  * (참고 3) 「개인정보 비식별 조치 방법」 참조

  ⇨ 비식별 조치가 완료되면 다음 단계의 조치 필요

● 〈 예시 〉 비식별 조치 방법 ●

처리기법	예시	세부기술
가명처리 (Pseudonymization)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대, 서울 거주, 국제대 재학	① 휴리스틱 가명화 ② 암호화 ③ 교환 방법
총계처리 (Aggregation)	• 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm	④ 총계처리 ⑤ 부분총계 ⑥ 라운딩 ⑦ 재배열
데이터 삭제 (Data Reduction)	• 주민등록번호 901206-1234567 → 90년대 생, 남자 • 개인과 관련된 날짜정보(합격일 등)는 연단위로 처리	⑧ 식별자 삭제 ⑨ 식별자 부분삭제 ⑩ 레코드 삭제 ⑪ 식별요소 전부삭제
데이터 범주화 (Data Suppression)	• 홍길동, 35세 → 홍씨, 30~40세	⑫ 감추기 ⑬ 랜덤 라운딩 ⑭ 범위 방법 ⑮ 제어 라운딩
데이터 마스킹 (Data Masking)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 홍○○, 35세, 서울 거주, ○○대학 재학	⑯ 임의 잡음 추가 ⑰ 공백과 대체

● 〈 예시 〉 비식별 조치 기법 적용 ●

원본데이터

주민등록번호	성별	입원날짜	연령	병명
770914–1234567	남	2015/06/23	39	독감
850930–1234567	남	2015/10/01	31	독감
710119–2345678	여	2014/01/21	45	고혈압
770619–2345678	여	2014/09/23	39	고혈압
830425–1234567	남	2015/04/16	33	간염
860804–2345678	여	2014/11/11	30	간염

비식별 데이터

① 데이터 삭제(주민등록번호)

~~주민등록번호~~	성별	입원날짜	연령	병명
	남	2015/06/23	39	독감
	남	2015/10/01	31	독감
	여	2014/01/21	45	고혈압
	여	2014/09/23	39	고혈압
	남	2015/04/16	33	간염
	여	2014/11/11	30	간염

② 데이터 마스킹(주민등록번호, 입원날짜), 총계처리(평균 연령)

주민등록번호	성별	입원날짜	연령	병명
7*****–1******	남	2015/**/**	35	독감
8*****–1******	남	2015/**/**	35	독감
7*****–2******	여	2014/**/**	35	고혈압
7*****–2******	여	2014/**/**	35	고혈압
8*****–1******	남	2015/**/**	35	간염
8*****–2******	여	2015/**/**	35	간염

2-③ 적정성 평가 단계 : k-익명성 모델 활용

적정성 평가 필요성

- 비식별 조치가 충분하지 않은 경우 공개 정보 등 다른 정보와의 결합, 다양한 추론 기법 등을 통해 개인이 식별될 우려

- 개인정보 보호책임자 책임 하에 외부전문가가 참여하는 「비식별 조치 적정성 평가단(이하, '평가단')」을 구성, 개인식별 가능성에 대한 엄격한 평가 필요

- 적정성 평가 시 프라이버시 보호 모델 중 k-익명성을 활용
  - k-익명성은 최소한의 평가수단이며, 필요시 추가적인 평가모델(ℓ -다양성, t-근접성) 활용
    * (참고 3) 「개인정보 비식별 조치 방법」 참조

넷플릭스 사례(2006, 미국)

- 온라인 영화대여 회사인 넷플릭스(Netflix)는 고객의 기호에 맞는 영화를 추천하는 알고리즘의 정확성을 높이기 위해 경연대회를 개최
  - 1999년 12월부터 2005년 12월까지 50만명의 이용자들이 영화에 대한 평점을 내린 1억건의 시청 이력 데이터를 공개
    ※ 사용자를 식별할 수 있는 이름 등은 삭제하였으나, 데이터 처리 내용을 연결하기 위해 독특한 식별자, 영화에 대한 평가 내용, 평가 일시 등을 공개

- 텍사스 대학의 한 그룹이 넷플릭스사가 공개한 시청 이력 데이터와 영화정보 사이트 IMDb(Internet Movie Database)에 공개된 사용자 리뷰를 결합하여 일부 개인을 식별해냄
  ※ IMDb는 웹 사이트 상에서 아이디와 평가점수를 게시

- 미국연방거래위원회(FTC)가 프라이버시에 관한 문제를 지적하여 제2회 경연은 중지됨

적정성 평가 절차

① **(기초자료 작성)** 개인정보처리자는 적정성 평가에 필요한 데이터 명세, 비식별 조치 현황, 이용기관의 관리 수준 등 기초자료 작성

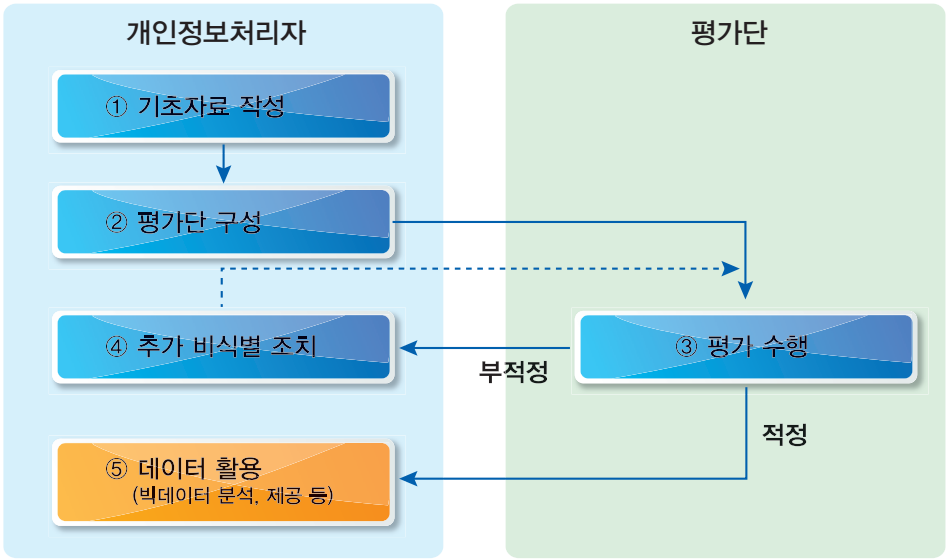
② **(평가단 구성)** 개인정보 보호책임자가 3명 이상으로 평가단을 구성(외부전문가는 과반수 이상)

③ **(평가 수행)** 평가단은 개인정보처리자가 작성한 기초자료와 k-익명성 모델을 활용하여 비식별 조치 수준의 적정성을 평가

④ **(추가 비식별 조치)** 개인정보처리자는 평가결과가 '부적정'인 경우 평가단의 의견을 반영하여 추가적인 비식별 조치 수행

⑤ **(데이터 활용)** 비식별 조치가 적정하다고 평가받은 경우에는 빅데이터 분석 등에 이용 또는 제공이 허용

● 비식별 조치에 대한 적정성 평가 절차 ●



① 기초자료 작성

- 개인정보처리자는 평가 대상 데이터 명세, 비식별 조치현황, 이용기관의 관리수준 등 적정성 평가에 필요한 기초자료를 작성

● 비식별 조치 적정성 평가에 필요한 기초 자료 ●

구분	기초자료	비 고
데이터 명세	• 데이터 특성(크기, 생성 및 관리 환경 등), 세부 항목별 명세, 원본 예시	필수사항
	• 비식별 조치된 평가 대상 데이터 셋 및 세부 항목별 명세	필수사항
비식별 조치 현황	• 비식별 조치에 적용한 기법 · 세부기술	필수사항
	• 평가 대상 데이터 셋에 대한 k-익명성 값 산출 결과	필수사항
이용기관의 관리수준	• 데이터 이용 기관의 이용 목적 및 방법, 이용기간, 데이터 접근 가능자 현황 등 활용에 관한 사항	필수사항
	• 데이터를 제공하는 경우 데이터를 제공받는 방법 및 데이터 보호를 위한 일련의 조치에 대한 현황	필수사항
	• 데이터 이용 및 제공과 관련이 있는 계약서 또는 협약서 사본 ※ 계약서가 없는 경우 그 사유 제시	필수사항
	• 데이터 이용 기관에서 보유하거나, 보유할 수 있는 개인정보 관련 데이터(세부 내용)에 관한 사항	선택사항
	• 데이터 이용기관의 개인정보보호 또는 정보보호 관련 인증서 사본	선택사항

② 평가단 구성

- 평가단은 해당 기관의 개인정보 보호책임자가 3명 이상의 관련 분야 전문가로 구성 (외부전문가를 과반수 이상으로 위촉*)

  * 외부전문가 위촉시 각 분야별 전문기관에서 운영하는 전문가 풀에서 법률 전문가, 비식별조치 기법 전문가를 각 1명 이상 활용(17~18쪽 참조)

- 평가단은 데이터 이용목적과 직접적인 이해관계가 없는 자로 구성

- 평가단의 단장은 외부전문가 중에서 호선으로 선출하며, 평가단 운영과 관련된 전반적인 사항을 관장

- 평가단은 착수회의를 포함해서 최소 2회 이상 운영

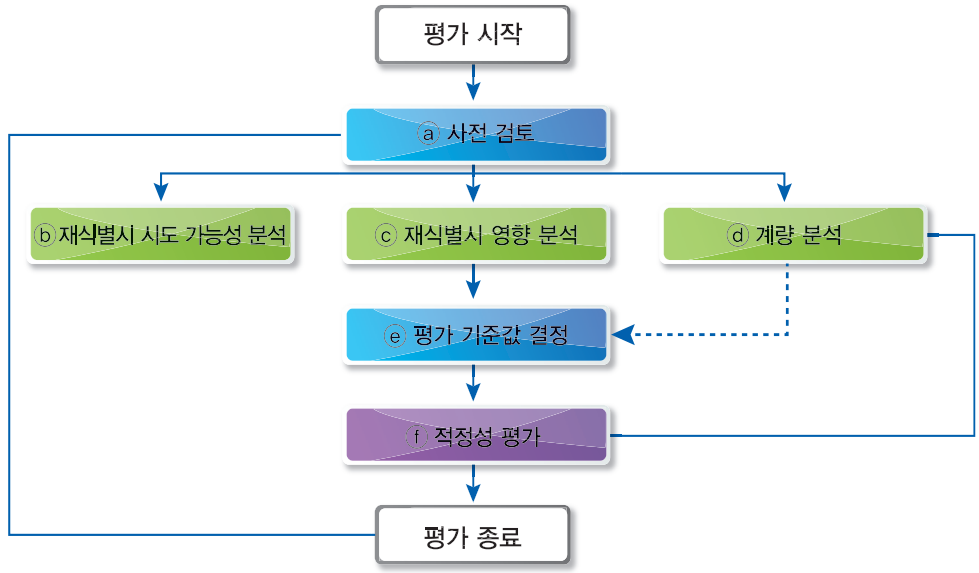
- 평가단은 필요한 경우 비식별 조치 관련 규정 마련 및 보완 등 권고

  – 컴퓨팅 환경의 발전, 이용 데이터 특성, 결합 가능한 정보의 입수 가능성 등을 고려, 필요한 경우 1년, 3년 등 재검토 일정을 제시

③ 평가 수행

- 평가단은 개인정보처리자가 제공한 기초자료와 k-익명성 모델 등을 활용하여 비식별 수준의 적정성 여부 평가

● 적정성 평가 수행 방법 ●



※ 「비식별 의료정보 공개 관리 가이드라인(캐나다, 2010.10월)」을 참조하여 절차 마련

ⓐ **(사전 검토)** 개인정보처리자가 제출한 기초자료와 인터뷰 등을 통해 평가대상 데이터의 개인 식별요소 포함 여부, 데이터 이용 목적, 비식별 조치 기법 등 검토

ⓑ **(재식별 시도 가능성)** 데이터를 이용 또는 제공받는 자의 재식별 의도와 능력, 개인정보 보호 수준 등 재식별 시도 가능성 분석

ⓒ **(재식별시 영향 분석)** 데이터가 의도적 또는 비의도적으로 재식별될 경우 정보주체 등에게 미칠 수 있는 영향 분석

ⓓ **(계량 분석)** 개인정보처리자가 제출한 k값의 정확성 여부 검증

ⓔ **(평가 기준값 결정)** 평가단에서 '재식별 시도 가능성', '재식별시 영향', '계량 분석' 결과와 데이터 이용 목적 등을 종합적으로 고려하여 평가 기준값(k-익명성 값) 결정

〈미국 교육부「프라이버시 보호 기술지원센터」의 안전도 기준〉

- 'k=3'은 안전도를 보장하는 최소한의 수준
- '5≦k≦10'은 안전도가 높은 수준

※ k-익명성 값은 데이터의 제공을 합법적으로 허용하기 위해 제시된 기준

ⓕ **(적정성 평가)** '평가 기준값'과 '계량 분석'에서 산출된 값을 비교하여 비식별 조치의 적정성 여부를 최종 결정

- 계량분석 결과의 k값이 4이고 평가 기준값이 3인 경우 '적정'으로 평가
- 계량분석 결과의 k값이 4이고 평가 기준값이 6인 경우 '부적정'으로 평가

– '적정'한 경우 ⇨ 데이터 이용 및 제공 가능

– '부적정'한 경우 ⇨ 추가적인 비식별 조치 및 재평가 수행

④ 추가 비식별 조치

- 개인정보처리자는 평가 결과가 '부적정'인 경우 평가단의 의견을 반영하여 해당 데이터에 대한 비식별 조치를 추가 실시
- 추가 비식별 조치가 완료된 경우에는 평가단에 비식별 조치가 적정히 수행되었는지에 대한 재평가를 요청

⑤ 데이터 활용

- 비식별 조치가 적정하다고 (재)평가받은 경우에는 해당 데이터를 빅데이터 분석 등에 이용하거나 제3자에게 제공이 허용
- 불특정 다수에게 공개하는 것은 식별 위험이 크므로 원칙적으로 금지

※「공공데이터의 제공 및 이용 활성화에 관한 법률」 등 법령에 따른 공개는 제외

- 데이터 이용 목적을 달성하거나 해당 데이터가 불필요하게 된 경우에는 지체 없이 파기 조치
- 데이터 활용 과정에서도 아래의 사후관리 단계의 조치사항을 준수하여야 비식별 정보로서 유효하게 활용 가능

2–④ 사후관리 단계

1 비식별 정보 안전 조치

○ 비식별 조치된 정보가 유출되는 경우 다른 정보와 결합하여 식별될 우려가 있으므로 필수적인 보호조치 이행

– **(관리적 보호조치)** 비식별 정보파일에 대한 관리 담당자 지정, 비식별 조치 관련 정보공유 금지, 이용 목적 달성시 파기 등의 조치가 필요함

– **(기술적 보호조치)** 비식별 정보파일에 대한 접근통제, 접속기록 관리, 보안 프로그램 설치 · 운영 등의 조치 필요

● 비식별 정보에 대한 관리적 · 기술적 보호조치 ●

구분	비식별 정보 보호 조치
관리적 보호조치	① 비식별 정보파일 관리담당자 지정 ② 비식별 정보파일 대장관리 ③ 원본정보 관리부서(기관)와 비식별 정보 관리부서(기관) 간 비식별 조치 관련 정보공유 금지 ④ 이용목적 달성시 지체없이 파기 ⑤ 비식별 정보파일 유출시 대응계획 수립
기술적 보호조치	⑥ 비식별 정보파일에 대한 접근권한 관리 및 접근통제 ⑦ 비식별 정보 보관시스템에 대한 접속기록 관리 ⑧ 악성 코드 방지 등을 위한 보안프로그램 설치 · 운영

○ 비식별 정보 유출 시 보호조치

– 유출 원인 분석 및 추가 유출 방지를 위한 관리적·기술적 보호조치

– 유출된 비식별 정보의 회수 · 파기

2 재식별 가능성 모니터링

- 비식별 정보를 이용하거나 제3자에게 제공하려는 사업자 등은 해당 정보의 재식별 가능성을 정기적으로 모니터링을 해야 함

- 모니터링 결과, 다음의 점검 항목 중 어느 하나에 해당되는 경우에는 추가적인 비식별 조치 강구

〈예시〉 재식별 가능성 모니터링 시 점검항목

구분	점검 항목
내부 요인의 변화	• 비식별 조치된 정보와 연계하여 재식별 우려가 있는 추가적인 정보를 수집하였거나 제공받은 경우
	• 데이터 이용과정에서 생성되는 정보가 비식별 정보와 결합해서 새로운 정보가 생성되는 경우
	• 이용부서에서 비식별 정보에 대한 비식별 수준을 당초보다 낮추어 달라고 하는 요구가 있는 경우
	• 신규 또는 추가로 구축되는 시스템이 비식별 정보에 대한 접근을 관리 · 통제하는 보안체계에 중대한 변화를 초래하는 경우
외부 환경의 변화	• 이용 중인 데이터에 적용된 비식별 조치 기법과 유사한 방법으로 비식별 조치한 사례가 재식별 되었다고 알려진 경우
	• 이용 중인 데이터에 적용된 비식별 기법과 기술을 무력화 하는 새로운 기술이 등장하거나 공개된 경우
	• 이용 중인 데이터와 새롭게 연계 가능한 정보가 출현하거나, 공개된 것으로 알려진 경우

- 비식별 정보를 제공 · 위탁한 자가 재식별 가능성을 발견한 경우에는 이를 즉시 그 정보를 처리하고 있는 자에게 통지하고 처리 중단 요구 및 해당 정보를 회수 · 파기하는 등 필요한 조치를 하여야 함

3 비식별 정보 제공 및 위탁계약 시 준수사항

- 비식별된 정보를 제3의 기관에 제공하거나, 처리 위탁하는 경우 재식별 위험관리에 관한 내용을 계약서에 포함
  - **(재식별 금지)** 비식별 정보를 제공받거나 처리를 위탁 받은 사업자 등은 다른 정보와 결합을 통해 재식별 시도가 금지됨을 명시
  - **(재제공 또는 재위탁 제한)** 비식별 정보를 제공하거나 처리를 위탁하는 자는 재제공 또는 재위탁 가능 범위를 정하여 계약서에 명시
  - **(재식별 위험 시 통지)** 재식별이 되거나 재식별 가능성이 높아지는 상황이 발생한 경우에는 데이터 처리 중지 및 비식별 정보 제공자 또는 위탁자에게 통지 의무 등 명시

계약서 특수조건 반영 내용 사례

제00조(재식별 금지)

① ○은 △으로부터 제공받은 비식별 정보를 ××한 목적으로 안전하게 이용하고, 이를 이용해서 개인을 재식별하기 위한 어떠한 행위도 하여서는 아니 된다.

② △으로부터 제공받은 정보를 ○이 제3자에게 제공하거나 처리를 위탁하고자 하는 경우에는 사전에 △의 동의를 얻어야 하며, 이 경우 ○는 재식별 방지를 위해 필요한 조치를 하여야 한다.

③ ○은 △으로부터 제공받은 정보가 재식별 되거나 재식별 가능성이 현저하게 높아지는 상황이 발생하면 즉시 해당 정보의 처리를 중단하고 관련 사항을 △에게 알리며, 필요한 협조를 하여야 한다.

④ ○은 제1항에서 제3항까지의 사항을 이행하지 않아 발생하는 모든 결과에 대해 형사 및 민사상 책임을 진다.

※ 비식별 정보를 제공받은 기업은 "○", 제공한 기업은 "△"로 표시

4 재식별 시 조치요령

- 비식별 정보가 재식별된 경우에는 신속하게 그 정보의 처리를 중단하고 해당 개인정보가 유출되지 않도록 필요한 조치를 하여야 함
- 재식별된 정보는 즉시 파기 조치하되, 해당 정보를 다시 활용하려면 비식별 조치 절차를 다시 거쳐야 함

Ⅲ 지원 및 관리체계

1 개인정보 비식별 조치 지원

지원 필요성

- 비식별 조치를 통해 개인정보를 안전하게 활용할 수 있는 지원체계 필요
  - 개인정보처리자가 수행하는 비식별 조치 적정성 평가 지원 등
- 비식별 조치에 필요한 컨설팅과 전문교육 등을 통해 중소기업 및 스타트업의 빅데이터 활용 지원
- 인공지능, 새로운 결합기술 출현 등에 따른 재식별 위험에 적극 대응

지원체계 및 지원내용

분야별 전문기관

- 각 소관부처 책임 하에 분야별 전문기관을 정하여 운영

  ※ 분야별 전문기관은 한국인터넷진흥원, 한국신용정보원, 금융보안원, 사회보장정보원, 한국정보화진흥원 중에서 소관부처가 공문으로 지정 · 공표하여 운영하고 필요시 추가 지정 가능

- 분야별 전문기관의 역할
  - 비식별 조치 적정성 평가단 풀(비식별 조치 기법 전문가, 법률 전문가 등) 구성·운영
  - 산업별로 필수적인 비식별 조치 이행 권고(k-익명성 수치 등)
    * 의료, 복지, 교육, 금융 · 신용, 통신, 유통, 공공 · 기타 분과
  - 비식별 조치 적정성 실태 점검 등
- '16년 8월 중 분야별 전문기관 지정 및 운영 개시

개인정보 비식별 지원센터

- 개인정보 보호 전담기관인 한국인터넷진흥원(KISA)에 「개인정보 비식별 지원센터」 설치 · 운영

- 개인정보 비식별 지원센터의 역할
  - 분야별 전문기관 운영 가이드라인 마련 및 실태 점검
  - 분야별 전문기관 실무협의회 운영
  - 분야별 평가단 풀 관리 및 교육, 중소기업 및 스타트업 컨설팅 · 교육
  - 「개인정보 비식별 조치 가이드라인」 업데이트 및 활용 지원
  - 국내외 관련 정책 · 기술 동향 조사 및 연구 등

- '16년 8월 중 설치 및 운영 개시

2 전문기관을 통한 기업 간 정보집합물 결합 지원

지원 필요성

- 빅데이터 분석에 활용하기 위해 서로 다른 사업자가 보유하고 있는 정보집합물을 결합하는 경우 개인별로 부여된 식별자가 매칭키로 사용
  - 이 경우, 정보주체를 알아볼 수 있는 식별자 그 자체를 매칭키로 사용하는 것은 현행법 위반 소지(개인정보 보호법 제18조, 개인정보의 목적 외 이용 · 제공 제한)

- 따라서, 정보집합물 간 결합 · 분석을 위해서는 결합 과정에서만 임시로 매칭키 역할을 하는 '임시 대체키'의 활용이 필요

- 임시 대체키를 활용한 결합을 허용하는 경우에도 무분별한 결합을 통한 개인정보 침해 소지를 방지하기 위해 전문기관(제3의 공공기관)에서만 결합을 하도록 하는 등 지원 및 관리체계 필요

지원 및 관리체계

- 기업 간 정보집합물 결합 지원은 분야별 전문기관에서 수행

- 전문기관 선택 기준
  - 산업내 기업간 결합은 해당 분야 전문기관에서 결합 지원
  - 이종산업 간 결합은 대량의 정보집합물을 결합하고자 하는 기업이 속해 있는 분야별 전문기관에서 수행
  - 당해 산업을 지원해 주는 전문기관이 없는 경우에는 한국인터넷진흥원 또는 한국정보화진흥원에서 지원

- 전문기관의 주요 역할 및 책임
  - 임시 대체키를 활용, 기업 간 정보집합물 결합 지원
  - 업무처리 전반에 있어 개인을 식별하려는 일체의 시도 금지
  - 정보집합물 결합 및 정보 제공 완료 후 모든 정보 지체 없이 파기

- 전문기관에 대한 세부 이용기준은 각 부처에서 마련 · 시행

정보집합물 결합 절차 및 유의사항

결합 절차

① A社와 B社가 같은 알고리즘을 적용하여 식별자를 임시 대체키로 전환하고, 결합대상 정보집합물도 비식별 조치 및 적정성 평가 수행

※ '임시 대체키' 생성시 동 대체키에 잡음을 추가하거나, 2개 이상의 식별자를 활용할 경우 식별자 중 일부를 조합하여 불법적 복호화 또는 원본 정보와 결합시에도 개인을 식별할 수 없도록 조치

② 비식별 조치된 정보를 전문기관에 제공 및 결합 요청

※ 이 경우 전문기관은 제공받은 비식별 정보를 통해 특정 개인 식별 불가

③ 임시 대체키를 활용, 전문기관에서 결합 수행

④ 임시 대체키 삭제

⑤ 결합 DB를 필요한 기업에게 제공(전문기관은 제공 후 파기 조치)

※ 임시 대체키가 삭제된 결합 DB가 제공되어 A와 B도 결합 DB를 통해 특정 개인의 식별이 어려움

● 임시 대체키를 통한 기업 간 정보집합물 결합 절차 ●

결합 시 유의사항

- A와 B는 분야별 전문기관과 임시 대체키 생성 알고리즘에 대한 정보공유 금지
- 임시 대체키 생성을 위해 주민등록번호를 활용하는 것은 금지
  (개인정보 보호법 제24조의2, 주민등록번호 처리의 제한)
- 다른 정보와의 결합을 위해 임시 대체키를 활용하는 경우, k-익명성 값은 임시 대체키를 제외하고 산출*

  * 임시 대체키를 제외하지 않으면, 'k=1'로 산출되어 객관적 평가 불가
- 전문기관은 결합 과정에서 재식별 발생시 해당 정보를 즉시 파기
- 결합 DB를 제공받은 기관은 이용 전에 반드시 적정성 평가 수행

3 재식별 시 법적 제재

형사처벌

○ 비식별 정보를 재식별하여 이용하거나 제3자에게 제공한 경우

> 예시 1 연구자에게 비식별 정보를 제공하면서 비식별 조치 요령을 공유하여 결과적으로 개인정보를 목적 외로 제공한 경우
>
> 예시 2 이름, 생년월일, 전화번호 등 주요 식별정보를 공개된 알고리즘으로 암호화하는 등 쉽게 재식별 될 수 있도록 하여 제3자에게 제공한 경우
>
> 예시 3 비식별 정보를 의도적으로 재식별하여 보관하고 있거나 1:1 마케팅 등에 활용한 경우

– 개인정보의 목적 외 이용 · 제공에 해당(개인정보 보호법 제18조제1항 위반, 정보통신망법* 제24조 및 제24조의2 위반, 신용정보법** 제32조 및 제33조 위반)

* 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, ** 「신용정보의 이용 및 보호에 관한 법률」

– 5년 이하의 징역 또는 5천만원 이하의 벌금

※ 정보통신망법 적용 사업자는 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

행정처분

○ 비식별 정보를 활용하여 재식별하고도 즉시 파기 조치하지 않고 보관하고 있는 경우

> 예시 비식별 정보를 제공받은 자가 업무처리 과정에서 특정 개인을 재식별하였으나 재식별된 정보를 즉시 파기하지 않고 보관하고 있는 경우

– 정보주체의 동의없이 개인정보를 수집한 경우에 해당(개인정보 보호법 제15조제1항 위반, 정보통신망법 제22조제1항 위반, 신용정보법 제15조제2항 위반)

– 5천만원 이하의 과태료가 부과

※ 정보통신망법 적용 사업자는 5년 이하 징역 또는 5천만원 이하 벌금형에 처해질 수 있으며 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

개인정보 비식별 조치 가이드라인

– 비식별 조치 기준 및 지원 · 관리체계 안내 –

참고

1. 비식별 정보의 산업적 활용(예시)
2. 국내외 동향
3. 개인정보 비식별 조치 방법
4. 비식별 조치 적정성 평가단 세부 평가수행 방법

참고 1 비식별 정보의 산업적 활용(예시)

기업 내부에서 비식별 정보 활용

업무처리 과정에서 수집한 고객정보, 거래내역, 민원처리 내역 등 개인정보가 포함된 각종 자료를 비식별 조치한 후 시장조사, 신상품 및 서비스 개발, 마케팅 전략 수립, 업무 프로세스 개선, 위험관리 등 다양한 용도로 분석 및 활용 가능
다만, 개인 식별을 전제로 하는 1:1 마케팅 용도로 사용할 수 없으며 재식별 시도는 금지

❶ ㅁㅁ공사는 고속도로 이용차량 빅데이터 분석을 통해 고객서비스 개선 전략 수립

▸ ㅁㅁ공사는 최근 5년간 톨게이트 진출입 데이터를 비식별 조치한 후 월별 · 시간대별 차량 평균속도, 상습 정체구간, 사고구간 및 원인 등 빅데이터 분석을 실시하여 도로 구조 개선 및 휴게공간 추가 설치 등 고객서비스 개선

❷ ○○통신사는 무선사업부 고객정보를 비식별 조치하여 단말기 판매부서에서 활용

▸ 단말기 판매부서는 요금제별 단말기 교환주기 및 단말기 선호 가격을 분석하여 단말기 판촉 전략을 수립

❸ △△보험사는 보험사기 사례 정보를 비식별 조치한 후 보험사기 방지시스템 개발

▸ 동 시스템을 통해 보험계약 체결, 유지, 보험금 지급 등 거래 전 단계에서 보험사기 징후를 자동으로 추출 · 예방함으로서, 보험사기 발생률 및 보험관리 비용 절감

다른 기업으로부터 비식별 정보를 제공받아 활용

본 가이드라인에 따라 비식별 조치한 정보는 제3자에게 제공할 수 있으며, 당해 비식별 정보를 제공받은 기업은 이를 시장조사, 신상품 및 서비스 개발, 마케팅 전략 수립 등 다양한 용도로 분석 및 활용 가능
다만, 이 경우 재식별 금지, 재식별 위험시 통지 등의 내용을 해당 비식별 정보 제공과 관련한 계약서에 반드시 포함하여야 하며, 제공받은 정보 또한 개인 식별을 전제로 하는 1:1 마케팅 용도로 사용할 수 없음

❶ ○○증권은 △△은행, ◇◇보험 등에서 비식별 조치한 자료를 제공받아 신상품 개발에 활용

▸ △△은행, ◇◇보험 등은 보유하고 있는 다양한 신용 정보를 비식별 조치한 후 ○○증권에게 제공

▸ ○○증권은 제공받은 자료를 빅데이터 분석하여 '로보어드바이저', 'ISA' 등 다양한 신상품 개발에 활용하고 국내 및 해외시장 개척을 추진

▸ '로보어드바이저'를 통해 개인이 문의할 경우 온라인 투자자문, 자산운용 상담 지원

❷ 신생 스타트업인 ◇◇사가 □□은행으로부터 비식별 정보를 제공받아 새로운 비즈니스 모델 개발에 활용

▸ □□은행은 보유하고 있는 학력 · 연령 · 성별 첫 직장, 이직경로, 연봉 등의 정보를 비식별 조치하여 신생 기업인 ◇◇사에 제공

▸ ◇◇사는 기존의 헤드헌팅 회사와 차별화된 '첫 직장부터 퇴직 후까지 커리어 관리 프로그램'을 제공하는 비즈니스 모델을 개발하여 활용

❸ ○○제약회사는 △△심사평가원으로부터 제공받은 비식별 정보를 ××신약개발 연구에 활용

▸ △△심사평가원이 특정 질병 환자의 연령과 성별에 따른 진료기록을 충분히 비식별 조치한 후, ○○제약회사에게 제공

▸ ○○제약회사는 해당 정보를 활용하여 ××병의 발병 원인 및 치유 원인을 분석하여 신약을 개발, 수입 약품 대비 20% 저렴한 가격으로 판매

❹ □□홈쇼핑은 ◇◇카드사로부터 구매금액 상위 10% 고객의 결제 내역에 대한 비식별 정보를 제공받아 우수고객 마케팅 전략 수립에 활용

▸ □□홈쇼핑과 ◇◇카드사는 고객 전화번호와 카드 결제정보를 각각 복원되지 않는 알고리즘으로 비식별 조치하여 A전문기관에 제공하고 A전문기관은 두 정보를 결합한 후, □□홈쇼핑에게 제공

▸ 비식별 조치된 고객의 결제정보를 통해 □□홈쇼핑은 우수고객이 선호하는 물품을 특정 시간대에 할인 행사를 실시하는 마케팅 전략 수립

참고 2 국내외 동향

1 미국

일반 동향

- 개인정보 보호에 관한 일반법이 없으며, 개별 법령에서 제한하지 않는 한 자유로운 데이터의 이용이 보장
  - 의료 · 교육 등 분야별로 개인정보 보호에 관한 개별 법령 운영 중
- 의료정보는 「건강보험 이전과 책임에 관한 법(HIPAA)」에 따른 「HIPAA 프라이버시 규칙」에서 비식별 조치 기준 제시
  ※ 비식별 조치된 의료정보는 제한 없이 이용 가능
- 「경제적 · 임상적 보건에 대한 건강 정보기술법(Health Information Technology for Economic and Clinical Health Act; HITECH Act)」에서는 비식별 조치된 건강정보에 대해 프라이버시 관련 규제 미적용
- 「가족의 교육적 권리 및 프라이버시 법(Family Educational Rights and Privacy Act; FERPA)」은 비식별 조치된 학생기록에 대해 별도의 동의없이 배포 가능(k-익명성 모델 활용)

HIPAA 프라이버시 규칙(HIPAA Privacy Rule)

- 「보호대상 의료정보의 비식별 가이드(Guidance on De-identification of Protected Health Information)」에 따라 비식별 조치된 의료정보를 규제대상에서 제외
  - 비식별 조치 방법에 따라 '전면적 규율면제' 또는 '부분적 규율면제' 방식 적용
- '전면적 규율면제'가 적용되는 비식별 조치방법에는 '전문가 결정방식'과 '세이프 하버 방식'이 있음
  - '전문가 결정방식'은 통계적, 과학적 원칙과 방법에 대한 지식과 경험을 보유한 전문가가 개인식별 위험 최소화 방법 적용

● 개인 위험 평가시 고려사항 ●

구 분	설 명
반복 가능성 (Replicability)	특정 개인과 관련하여 반복적으로 계속되는 정보(eg, 생일 등)는 개인식별 위험이 높다고 판별
데이터 소스 이용가능성 (Data Source Availability)	외부에 많이 공개되어 있는 정보는 덜 공개된 정보보다 상대적으로 개인식별에 활용될 가능성이 높음
구별 가능성 (Distinguishability)	특정인을 구별할 수 있는 정보(eg, 주소정보)는 그렇지 않은 정보(생년)보다 상대적으로 더 위험함

– '세이프 하버 방식'은 이름, 주소정보 등 18가지 주요 식별자*를 제거하여 개인식별이 가능하지 못하도록 하는 방식

* 18가지 식별자 : ①이름 ②주소정보 ③개인과 직접 관련된 날짜정보(생일, 합격일 등) ④전화번호 ⑤팩스번호 ⑥이메일 주소 ⑦사회보장번호 ⑧의료기록번호 ⑨건강보험번호 ⑩계좌번호 ⑪자격취득번호 ⑫자동차번호 ⑬각종 장비 식별번호 ⑭URL정보 ⑮IP주소 ⑯생체정보 ⑰전체 얼굴사진과 이와 유사한 이미지 ⑱기타 특이한 식별 번호 또는 코드

○ '부분적 규율면제'는 위의 18가지 식별자 중 '③ 날짜정보', '⑱ 기타 식별번호 또는 코드' 외의 16개 식별자를 제거한 경우에 적용

– 데이터 제공자와 제공받는 자 간에 데이터 이용 및 제공목적 등을 담은 계약을 체결하여 진행

2 EU

EU 동향

○ EU 역내 개인정보 보호를 규율하는 일반규정인 「EU 개인정보 보호 지침*(EU Data Protection Directive)」 서문에서는 익명화된(Anonymized) 정보는 동 지침의 규제 대상이 아니라고 명시

* 지침은 각 회원국이 국내법을 제정 · 시행하는데 적용되는 가이드로서 강제성은 없음

○ 지침에는 가명처리된(Pseudonymized) 정보는 과학적 연구, 역사연구, 통계 목적으로 사용 가능함을 명시

– 구체적인 처리 기준 등 자세한 사항은 회원국이 정하도록 함

○ 최근 EU에서 단일한 개인정보 보호법(General Data Protection Regulation; GDPR)이 EU 의회를 통과('16.4.14., 2년 후 시행 예정)

– 기존 지침의 가명정보 규정이 법적 구속력이 있는 GDPR에 명문화

– 다만, 가명정보를 동의없이 처리할 수 있는 목적의 범위가 공익, 과학적 연구, 역사연구, 통계 목적으로 일부 변경

영국 사례

- 영국 정보보호 커미셔너(ICO)는 EU 지침 서문에 근거하여 '12년에 EU 최초로 익명화 규약*을 출간

  * ICO, "Anonymisation: managing data protection risk code of practice, 2012"

  – 요구되는 익명화의 정도는 식별 위험성이 '0(zero) 수준'은 아니나, 식별 위험성이 매우 낮은(remote) 수준이어야 함을 명시

- 식별 위험성의 판단 기준으로 '합리적 가능성(reasonably likely test)' 기준을 채택

  – 식별의 위험성이 합리적으로 가능할 경우에는 규제의 대상이 되는 개인정보에 해당하며 이 기준은 EU 지침과 동일

3 일본

- 최근 일본 정부는 IT종합전략본부를 중심으로 개인정보의 합리적 활용을 촉진하기 위해 개인정보 보호법 개정('15.9월 개정, '17.1월 시행)

  – 개인정보의 빅데이터 활용 확대를 위해 익명가공정보 개념 신설

  – 익명가공정보는 복원 불가능도록 안전 조치를 함을 전제로 정보주체의 동의없이 활용할 수 있도록 허용

  – 익명가공정보 취급 사업자*에게 일정한 기술적 · 관리적 조치 의무** 부여

  * 특정의 익명가공정보를 전자장치를 이용하여 검색할 수 있도록 체계적으로 구성하여 다른 사업자에게 판매 또는 제공하는 자

  ** 복원불능 정보 작성, 정보누설 방지, 정보항목 공개, 제3자 제공 시 공표, 식별행위 금지, 안전조치 의무 등 부담

- 일본 정부는 관계 전문가와 함께 비식별 가이드라인 마련 추진 중

  – 이와 관련, 전문가들은 '완전한 익명화'는 있을 수 없음을 인정하고, 익명화의 수준을 단계별로 구분 · 제시하는 방안 논의 중

  – 그중 익명화 수준을 가장 높도록 조치하기 위한 방법으로 k–익명성 모델을 활용하는 방안을 검토하고 있음

> 우리나라의 경우에는 k–익명성 모델을 기본적으로 적용하고, 필요시 추가적인 평가모델인 ℓ –다양성 모델과 t–근접성 모델까지 적용

4 우리나라

구 분	공공정보 개방 · 공유에 따른 개인정보 보호지침	개인정보 비식별화에 대한 적정성 자율평가 안내서	빅데이터 개인정보보호 가이드라인	빅데이터 활용을 위한 개인정보 비식별화 기술 활용 안내서
발간	2013.9	2014.12	2014.12	2015.6
주관 부처	행정자치부	행정자치부	방송통신위원회	미래창조과학부
대 상	공공	공공, 민간	민간	공공, 민간
목적	공공정보 개방 · 공유 등에 따른 개인정보 보호조치 요령 안내	개인정보 비식별화 적정성 평가, 재식별 위험 관리 및 조치요령 안내	빅데이터 관련 개인정보 보호법령 적용 방안 설명	빅데이터 활용을 위한 비식별화 기술 활용방법 및 관련 법규 안내
주요 내용	(1단계) 공공정보 개방 · 공유 근거 확인 (2단계) 개인식별 요소 제거 (3단계) 개인식별 가능성 검토 (4단계) 비식별 기법 및 재식별 가능성에 관한 주기적 모니터링 실시	개인정보가 포함된 정보는 개인정보 식별요소 제거를 통해 개인을 식별할 수 없는 형태로 정보를 변경 후 이용 재식별 위험에 대한 관리적 조치 및 재식별시 대응 조치 공공정보 개방 · 공유 등에 따른 개인정보 보호지침과 유사한 조치 및 프라이버시 보호모델에 따른 검토를 하도록 함	공개된 정보, 이용내역 정보, 생성된 정보는 비식별화 조치 후 처리 비식별화 조치한 경우 이용자의 동의 없이 수집 · 이용 가능 비식별 조치 후 저장 시 보호조치 필요 비식별화 조치된 개인정보는 이용자 동의 없이 제3자 제공 가능	개인식별이 가능한 정보는 삭제 다른 정보와 결합으로 재식별될 위험 최소화 및 사후관리 철저 가명처리, 총계처리, 데이터 값 삭제, 범주화, 데이터 마스킹 등 18가지 비식별화 기술 및 적용사례 제시

참고 3 개인정보 비식별 조치 방법

1 개요

일반적 기법 : 개인 식별요소 삭제 방법

처리기법	예시	세부기술
가명처리 (Pseudonymization)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대, 서울 거주, 국제대 재학	① 휴리스틱 가명화 ② 암호화 ③ 교환 방법
총계처리 (Aggregation)	• 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm	④ 총계처리 ⑤ 부분총계 ⑥ 라운딩 ⑦ 재배열
데이터 삭제 (Data Reduction)	• 주민등록번호 901206-1234567 → 90년대 생, 남자 • 개인과 관련된 날짜정보(합격일 등)는 연단위로 처리	⑧ 식별자 삭제 ⑨ 식별자 부분삭제 ⑩ 레코드 삭제 ⑪ 식별요소 전부삭제
데이터 범주화 (Data Suppression)	• 홍길동, 35세 → 홍씨, 30~40세	⑫ 감추기 ⑬ 랜덤 라운딩 ⑭ 범위 방법 ⑮ 제어 라운딩
데이터 마스킹 (Data Masking)	• 홍길동, 35세, 서울 거주, 한국대 재학 → 홍○○, 35세, 서울 거주, ○○대학 재학	⑯ 임의 잡음 추가 ⑰ 공백과 대체

프라이버시 보호 모델 : 재식별 가능성 검토 기법 * k, ℓ, t값은 전문가 등이 검토하여 마련

기법	의미	적용례
k-익명성	• 특정인임을 추론할 수 있는지 여부를 검토, 일정 확률수준 이상 비식별 되도록 함	• 동일한 값을 가진 레코드를 k개 이상으로 함. 이 경우 특정 개인을 식별할 확률은 1/k임
ℓ-다양성	• 특정인 추론이 안된다고 해도 민감한 정보의 다양성을 높여 추론 가능성을 낮추는 기법	• 각 레코드는 최소 l개 이상의 다양성을 가지도록 하여 동질성 또는 배경지식 등에 의한 추론 방지
t-근접성	• ℓ-다양성 뿐만 아니라, 민감한 정보의 분포를 낮추어 추론 가능성을 더욱 낮추는 기법	• 전체 데이터 집합의 정보 분포와 특정 정보의 분포 차이를 t이하로 하여 추론 방지

2 일반적 기법

가명처리(Pseudonymization)

- (개념) 개인 식별이 가능한 데이터를 직접적으로 식별할 수 없는 다른 값으로 대체하는 기법
- (대상) 성명, 기타 고유특징(출신학교, 근무처 등)
- (장점) 데이터의 변형 또는 변질 수준이 적음
- (단점) 대체 값 부여 시에도 식별 가능한 고유 속성이 계속 유지

실무적용 방법

① **휴리스틱 가명화(Heuristic Pseudonymization)**

– 식별자에 해당하는 값들을 몇 가지 정해진 규칙으로 대체하거나 사람의 판단에 따라 가공하여 자세한 개인정보를 숨기는 방법

(ex) 성명을 홍길동, 임꺽정 등 몇몇 일반화된 이름으로 대체하여 표기하거나 소속기관명을 화성, 금성 등으로 대체하는 등 사전에 규칙을 정하여 수행

– 식별자의 분포를 고려하거나 수집된 자료의 사전 분석을 하지 않고 모든 데이터를 동일한 방법으로 가공하기 때문에 사용자가 쉽게 이해하고 활용 가능

– 활용할 수 있는 대체 변수에 한계가 있으며, 다른 값으로 대체하는 일정한 규칙이 노출되는 취약점이 있음. 따라서 규칙 수립 시 개인을 쉽게 식별할 수 없도록 세심한 고려 필요

– 적용정보 : 성명, 사용자 ID, 소속(직장)명, 기관번호, 주소, 신용등급, 휴대전화번호, 우편번호, 이메일 주소 등

② **암호화(Encryption)**

– 정보 가공시 일정한 규칙의 알고리즘을 적용하여 암호화함으로써 개인정보를 대체하는 방법, 통상적으로 다시 복호가 가능하도록 복호화 키(key)를 가지고 있어서 이에 대한 보안방안도 필요

– 일방향 암호화(one-way encryption 또는 hash)를 사용하는 경우는 이론상 복호화가 원천적으로 불가능

※ 일방향 암호화는 개인정보의 식별성을 완전히 제거하는 것으로, 양방향 암호화에 비해 더욱 안전하고 효과적인 비식별 기술에 해당

– 적용정보 : 주민등록번호, 여권번호, 의료보험번호, 외국인등록번호, 사용자 ID, 신용카드번호, 생체정보 등

③ **교환 방법(Swapping)**

– 기존의 데이터베이스의 레코드를 사전에 정해진 외부의 변수(항목)값과 연계하여 교환

– 적용정보 : 사용자 ID, 요양기관번호, 기관번호, 나이, 성별, 신체정보(신장, 혈액형 등), 소득, 휴대전화번호, 주소 등

총계처리(Aggregation)

- (개념) 통계값(전체 혹은 부분)을 적용하여 특정 개인을 식별할 수 없도록 함
- (대상) 개인과 직접 관련된 날짜 정보(생일, 자격 취득일), 기타 고유 특징(신체정보, 진료기록, 병력정보, 특정소비기록 등 민감한 정보)
- (장점) 민감한 수치 정보에 대하여 비식별 조치가 가능하며, 통계분석용 데이터 셋 작성에 유리함
- (단점) 정밀 분석이 어려우며, 집계 수량이 적을 경우 추론에 의한 식별 가능성 있음

실무적용 방법

④ **총계처리(Aggregation)**

– 데이터 전체 또는 부분을 집계(총합, 평균 등)

※ 단, 데이터 전체가 유사한 특징을 가진 개인으로 구성되어 있을 경우 그 데이터의 대푯값이 특정 개인의 정보를 그대로 노출시킬 수도 있으므로 주의

(예시) 집단에 소속된 전체 인원의 평균 나이값을 구한 후 각 개인의 나이값을 평균 나이값(대푯값)으로 대체하거나 해당 집단 소득의 전체 평균값을 각 개인의 소득값으로 대체

– 적용정보 : 나이, 신장, 소득, 카드사용액, 유동인구, 사용자수, 제품 재고량, 판매량 등

⑤ **부분총계(Micro Aggregation)**

– 데이터 셋 내 일정부분 레코드만 총계 처리함. 즉, 다른 데이터 값에 비하여 오차 범위가 큰 항목을 통계값(평균 등)으로 변환

(예시) 다양한 연령대의 소득 분포에 있어서 40대의 소득 분포 편차가 다른 연령대에 비하여 매우 크거나 특정 소득 구성원을 포함하고 있을 경우, 40대의 소득만 선별하여 평균값을 구한 후 40대에 해당하는 각 개인의 소득값을 해당 평균값으로 대체

– 적용정보 : 나이, 신장, 소득, 카드사용액 등

⑥ **라운딩(Rounding)**

– 집계 처리된 값에 대하여 라운딩(올림, 내림, 사사오입) 기준을 적용하여 최종 집계 처리하는 방법으로, 일반적으로 세세한 정보보다는 전체 통계정보가 필요한 경우 많이 사용

(예시) 23세, 41세, 57세, 26세, 33세 등 각 나이값을 20대, 30대, 40대, 50대 등 각 대표 연령대로 표기하거나 3,576,000원, 4,210,000원 등의 소득값을 일부 절삭하여 3백만원, 4백만원 등으로 집계 처리하는 방식

– 적용정보 : 나이, 신장, 소득, 카드지출액, 유동인구, 사용자 수 등

⑦ **재배열(Rearrangement)**

– 기존 정보값은 유지하면서 개인이 식별되지 않도록 데이터를 재배열하는 방법으로, 개인의 정보를 타인의 정보와 뒤섞어서 전체 정보에 대한 손상 없이 특정 정보가 해당 개인과 연결되지 않도록 하는 방법

(예시) 데이터 셋에 포함된 나이, 소득 등의 정보를 개인별로 서로 교환하여 재배치하게 되면 개인별 실제 나이와 소득과 다른 비식별 자료를 얻게 되지만, 전체적인 통계 분석에 있어서는 자료의 손실 없이 분석을 할 수 있는 장점이 있음

– 적용정보 : 나이, 신장, 소득, 질병, 신용등급, 학력 등

데이터 삭제(Data Reduction)

- (개념) 개인 식별이 가능한 데이터 삭제 처리
- (대상) 개인을 식별 할 수 있는 정보(이름, 전화번호, 주소, 생년월일, 사진, 고유식별정보(주민등록번호, 운전면허번호 등), 생체정보(지문, 홍채, DNA 정보 등), 기타(등록번호, 계좌번호, 이메일주소 등))
- (장점) 개인 식별요소의 전부 및 일부 삭제 처리가 가능
- (단점) 분석의 다양성과 분석 결과의 유효성 · 신뢰성 저하

실무적용 방법

⑧ **식별자 삭제**

– 원본 데이터에서 식별자를 단순 삭제하는 방법

(예시) 성명, 생년월일(yy–mm–dd)이 나열되어 있는 경우 분석 목적에 따라 생년월일을 생년(yy)으로 대체 가능하다면 월일(mm–dd) 값은 삭제

※ 이때 남아 있는 정보 그 자체로도 분석의 유효성을 가져야 함과 동시에 개인을 식별할 수 없어야 하며, 인터넷 등에 공개되어 있는 정보 등과 결합하였을 경우에도 개인을 식별할 수 없어야 함

– 적용정보 : 성명, 전화번호, 계좌번호, 카드번호, 요양기관번호, 이메일 주소 등

⑨ **식별자 부분삭제**

– 식별자 전체를 삭제하는 방식이 아니라, 해당 식별자의 일부를 삭제하는 방법

(예시) 상세 주소의 경우 부분 삭제를 통하여 대표지역으로 표현
(서울특별시 송파구 가락본동 78번지 → 서울시 송파구)

– 수치 또는 텍스트 데이터 등에도 폭넓게 활용 가능('⑫감추기'는 주로 수치데이터에 적용)

– 적용정보 : 주소, 위치정보(GPS), 전화번호, 계좌번호 등

⑩ **레코드 삭제(Reducing Records)**

– 다른 정보와 뚜렷하게 구별되는 레코드 전체를 삭제하는 방법

(예시) 소득이 다른 사람에 비하여 뚜렷이 구별되는 값을 가진 정보는 해당 정보 전체를 삭제

– 이 방법은 통계분석에 있어서 전체 평균에 비하여 오차범위를 벗어나는 자료를 제거할 때에도 사용 가능

– 적용정보 : 키, 소득, 질병, 카드지출액 등

⑪ **식별요소 전부삭제**

– 식별자뿐만 아니라 잠재적으로 개인을 식별할 수 있는 속성자까지 전부 삭제하여 프라이버시 침해 위험을 줄이는 방법

(예시) 연예인 · 정치인 등의 가족정보(관계정보), 판례 및 보도 등에 따라 공개되어 있는 사건과 관련되어 있음을 알 수 있는 정보 등 잠재적 식별자까지 사전에 삭제함으로써 연관성 있는 정보의 식별 및 결합을 예방

– 개인정보 유출 가능성을 최대한 줄일 수 있지만 데이터 활용에 필요한 정보까지 사전에 모두 없어지기 때문에 데이터의 유용성이 낮아지는 문제 발생

– 적용정보 : 나이, 소득, 키, 몸무게 등 개별적으로는 단순한 정보이지만 분석 목적에 따라 추후 개인 식별이 가능성이 있다고 판단되는 정보

데이터 범주화(Data Suppression)

- (개념) 특정 정보를 해당 그룹의 대푯값으로 변환(범주화)하거나 구간값으로 변환(범주화)하여 개인 식별을 방지
- (대상) 개인을 식별할 수 있는 정보(주소, 생년월일, 고유식별정보(주민등록번호, 운전면허번호 등), 기관 · 단체 등의 이용자 계정(등록번호, 계좌번호))
- (장점) 통계형 데이터 형식이므로 다양한 분석 및 가공 가능
- (단점) 정확한 분석결과 도출이 어려우며, 데이터 범위 구간이 좁혀질 경우 추론 가능성 있음

실무적용 방법

⑫ **감추기**

– 명확한 값을 숨기기 위하여 데이터의 평균 또는 범주값으로 변환하는 방식

– 단, 특수한 성질을 지닌 개인으로 구성된 단체 데이터의 평균이나 범주값은 그 집단에 속한 개인의 정보를 쉽게 추론할 수 있음

(예시) 간염 환자 집단임을 공개하면서 특정인물 '갑'이 그 집단에 속함을 알 수 있도록 표시하는 것은 '갑'이 간염 환자임을 공개하는 것과 마찬가지임

⑬ **랜덤 라운딩(Random Rounding)**

– 수치 데이터를 임의의 수 기준으로 올림(round up) 또는 내림(round down)하는 기법

– '⑥ 라운딩(rounding)과 달리 수치 데이터 이외의 경우에도 확장 적용 가능

(예시) 나이, 우편번호 등과 같은 수치 정보로 주어진 식별자는 일의 자리, 십의 자리 등 뒷자리 수를 숨기고 앞자리 수만 나타내는 방법(나이 : 42세, 45세 → 40대로 표현)

– 적용정보 : 나이, 소득, 카드지출액, 우편번호, 유동인구, 사용자 등

⑭ **범위 방법(Data Range)**

– 수치데이터를 임의의 수 기준의 범위(range)로 설정하는 기법으로, 해당 값의 범위(range) 또는 구간(interval)으로 표현

(예시) 소득 3,300만원을 소득 3,000만원~4,000만원으로 대체 표기

– 적용정보 : 서비스 이용 등급, 처방정보(횟수, 기간 등), 위치정보, 유동인구, 사용자 수, 분석 시간/기간 등

⑮ **제어 라운딩(Controlled Rounding)**

– '⑬랜덤 라운딩' 방법에서 어떠한 특정값을 변경할 경우 행과 열의 합이 일치하지 않는 단점 해결을 위해 행과 열이 맞지 않는 것을 제어하여 일치시키는 기법

– 그러나 컴퓨터 프로그램으로 구현하기 어렵고 복잡한 통계표에는 적용하기 어려우며, 해결할 수 있는 방법이 존재하지 않을 수 있어 아직 현장에서는 잘 사용하지 않음

– 적용정보 : 나이, 키, 소득, 카드지출액, 위치정보 등

데이터 마스킹(Data Masking)

- (개념) 데이터의 전부 또는 일부분을 대체값(공백, 노이즈 등)으로 변환
- (대상) 쉽게 개인을 식별할 수 있는 정보(이름, 전화번호, 주소, 생년월일, 사진, 고유식별정보(주민등록번호, 운전면허번호 등), 기관 · 단체 등의 이용자 계정(등록번호, 계좌번호, 이메일 주소 등))
- (장점) 개인 식별 요소를 제거하는 것이 가능하며, 원 데이터 구조에 대한 변형이 적음
- (단점) 마스킹을 과도하게 적용할 경우 데이터 필요 목적에 활용하기 어려우며 마스킹 수준이 낮을 경우 특정한 값에 대한 추론 가능

실무적용 방법

⑯ **임의 잡음 추가(Adding Random Noise)**

– 개인 식별이 가능한 정보에 임의의 숫자 등 잡음을 추가(더하기 또는 곱하기)하는 방법

(예시) 실제 생년월일에 6개월의 잡음을 추가할 경우, 원래의 생년월일 데이터에 1일부터 최대 6개월의 날짜가 추가되어 기존의 자료와 오차가 날 수 있도록 적용

– 지정된 평균과 분산의 범위 내에서 잡음이 추가되므로 원 자료의 유용성을 해치지 않으나, 잡음값은 데이터 값과는 무관하기 때문에, 유효한 데이터로 활용하기 곤란

– 적용정보 : 사용자 ID, 성명, 생년월일, 키, 나이, 병명 코드, 전화번호, 주소 등

⑰ **공백(blank)과 대체(impute)**

– 특정 항목의 일부 또는 전부를 공백 또는 대체문자(' * ', ' _ ' 등이나 전각 기호)로 바꾸는 기법

(예시) 생년월일 '1999-09-09' ⇒ '19 – – ' 또는 '19**-**-**'

– 적용정보 : 성명, 생년월일, 전화번호, 주소, 사용자 ID 등

3 프라이버시 보호 모델

k-익명성(k-anonymity) : 프라이버시 보호를 위한 기본 모델

○ 공개된 데이터에 대한 연결공격(linkage attack) 등 취약점*을 방어하기 위해 제안된 프라이버시 보호 모델

＊ 공개 데이터의 취약점

- **개인정보를 포함한 공개 데이터**
  - 일반적으로 활용하는 데이터에는 이름, 주민등록번호 등과 같이 개인을 직접 식별할 수 있는 데이터는 삭제(예: 〈표 1〉)
  - 그러나 활용 정보의 일부가 다른 공개되어 있는 정보 등과 결합하여 개인을 식별하는 문제(연결공격)가 발생 가능(예: 〈표 2〉)
- **연결공격(linkage attack)**
  - 예를 들어, 〈표 1〉의 의료데이터가 〈표 2〉의 선거인명부와 지역 코드, 연령, 성별에 의해 결합되면, 개인의 민감한 정보인 병명이 드러날 수 있음

    (ex) 김민준 (13053, 28, 남자)→ 환자 레코드 1번→ 전립선염
  - 미국 매사추세츠 주, '선거인명부'와 '공개 의료데이터'가 결합하여 개인의 병명 노출 사례

○ (정의) 주어진 데이터 집합에서 같은 값이 적어도 k개 이상 존재하도록 하여 쉽게 다른 정보로 결합할 수 없도록 함

- 데이터 집합의 일부를 수정하여 모든 레코드가 자기 자신과 동일한(구별되지 않는) k-1개 이상의 레코드를 가짐
- 예를 들어, 〈표 1〉의 의료 데이터가 비식별 조치된 〈표 3〉에서 1~4, 5~8, 9~12 레코드는 서로 구별되지 않음

● 〈표 1〉 공개 의료데이터 사례 ●

구분	지역 코드	연령	성별	질병
1	13053	28	남	전립선염
2	13068	21	남	전립선염
3	13068	29	여	고혈압
4	13053	23	남	고혈압
5	14853	50	여	위암
6	14853	47	남	전립선염
7	14850	55	여	고혈압
8	14850	49	남	고혈압
9	13053	31	남	위암
10	13053	37	여	위암
11	13068	36	남	위암
12	13068	35	여	위암

● 〈표 2〉 선거인명부 사례 ●

구분	이름	지역코드	연령	성별
1	김민준	13053	28	남
2	박지훈	13068	21	남
3	이지민	13068	29	여
4	최현우	13053	23	남
5	정서연	14853	50	여
6	송현준	14850	47	남
7	남예은	14853	55	여
8	성민재	14850	49	남
9	윤건우	13053	31	남
10	손윤서	13053	37	여
11	민우진	13068	36	남
12	허수빈	13068	35	여

● 〈표 3〉 k-익명성 모델에 의해 비식별된 의료데이터 사례 ●

구분	지역 코드	연령	성별	질병	비고
1	130**	< 30	*	전립선염	다양한 질병이 혼재되어 안전
2	130**	< 30	*	전립선염	
3	130**	< 30	*	고혈압	
4	130**	< 30	*	고혈압	
5	1485*	> 40	*	위암	다양한 질병이 혼재되어 안전
6	1485*	> 40	*	전립선염	
7	1485*	> 40	*	고혈압	
8	1485*	> 40	*	고혈압	
9	130**	3*	*	위암	모두가 동일 질병(위암)으로 취약
10	130**	3*	*	위암	
11	130**	3*	*	위암	
12	130**	3*	*	위암	

※ '∗' 표시는 임의의 글자를 나타낸다. 가령, 지역코드 '130**'은 '13000~13099' 범위 안에 존재하는 하나의 지역코드 값을 의미한다.

- 따라서, 비식별된 데이터 집합에서는 공격자가 정확히 어떤 레코드가 공격 대상인지 알아낼 수 없음

  ※ (예시) 〈표 2〉 김민준→ 〈표 3〉 레코드 1~4→ 전립선염 또는 고혈압

- 여기서, 같은 속성자 값들로 비식별된 레코드들의 모임을 '동일 속성자 값 집합(equivalent class, 이하 동질 집합)'이라고 함

  ※ (예시) 〈표 3〉 레코드1~4, 5~8, 9~12

ℓ-다양성(ℓ-diversity) : k-익명성의 취약점*을 보완한 프라이버시 보호 모델

- k-익명성에 대한 두 가지 공격, 즉 동질성 공격 및 배경지식에 의한 공격을 방어하기 위한 모델
- (정의) 주어진 데이터 집합에서 함께 비식별되는 레코드들은 (동질 집합에서) 적어도 ℓ개의 서로 다른 민감한 정보를 가져야 함
  - 비식별 조치 과정에서 충분히 다양한(ℓ개 이상) 서로 다른 민감한 정보를 갖도록 동질 집합을 구성
- 정보가 충분한 다양성을 가지므로 다양성의 부족으로 인한 공격에 방어가 가능하고, 배경지식으로 인한 공격에도 일정 수준의 방어능력

* k-익명성의 취약점

- **취약점 1. 동질성 공격 (Homogeneity attack)**
  - k-익명성에 의해 레코드들이 범주화 되었더라도 일부 정보들이 모두 같은 값을 가질 수 있기 때문에 데이터 집합에서 동일한 정보를 이용하여 공격 대상의 정보를 알아내는 공격
  - 〈표 3〉에서 범주화의 기초가 되는 정보(지역코드, 연령, 성별)에 대해서는 여러 다양한 값들이 혼재되어 있어서 연결 공격에 의한 식별이 어렵지만, 이 정보와 연결된 정보(질병)는 'k-익명성'의 기초가 아니기 때문에 발생할 수 있는 현상
  - 예를 들어, 〈표 3〉에서 레코드 9~12의 질병정보는 모두 '위암'이므로 k-익명성 모델이 적용되었음에도 불구하고 그 질병정보가 직접적으로 노출됨

- **취약점 2. 배경지식에 의한 공격 (Background knowledge attack)**
  - 주어진 데이터 이외의 공격자의 배경 지식을 통해 공격 대상의 민감한 정보를 알아내는 공격
  - 〈표 2〉와 〈표 3〉에서 공격자가 '이지민'의 질병을 알아내려고 하면 정보의 결합(13068, 29, 여)에 따라 '이지민'은 〈표 3〉의 1~4 레코드 중 하나이며 질병은 전립선염 또는 고혈압임을 알 수 있음
  - 이 때, '여자는 전립선염에 걸릴 수 없다'라는 배경 지식에 의해 공격 대상 '이지민'의 질병은 고혈압으로 쉽게 추론 가능함

- **k-익명성의 취약점의 원인**
  - 다양성의 부족 (lack of diversity)
    - 비식별 조치 할 때 정보의 다양성을 고려하지 않음
    - 동일한 정보를 가진 (다양하지 않은) 레코드가 비식별되어 하나의 '동질 집합'으로 구성될 경우 동질성 공격에 무방비
  - 강한 배경지식 (strong background knowledge)
    - k-익명성은 '여자는 전립선염에 걸리지 않는다' 또는 '남자는 자궁암에 걸리지 않는다'와 같은 공격자의 배경지식을 고려하지 않아 이를 이용한 공격에 취약

- 예를 들어, 〈표 4〉에서 모든 동질 집합은 3–다양성(ℓ =3)을 통해 비식별되어 3개 이상의 서로 다른 정보를 가짐
  - 〈표 3〉과 같이 동일한 질병으로만 구성된 동질 집합이 존재하지 않음
  - 공격자가 질병에 대한 배경지식(예: 여자는 전립선염에 걸리지 않음)이 있더라도 어느 정도의 방어력을 가지게 됨(예: 여성 이지민이 속한 동질 집합 2, 3, 11, 12에서 전립선염을 제외하더라도 고혈압, 위암 중 어느 질병이 이지민의 것인지 여전히 알 수 없음)

〈표 4〉 ℓ –다양성 모델에 의해 비식별된 의료데이터의 예

구분	지역 코드	연령	성별	질병	비고
1	1305*	≤ 40	*	전립선염	다양한 질병이 혼재되어 안전
4	1305*	≤ 40	*	고혈압	
9	1305*	≤ 40	*	위암	
10	1305*	≤ 40	*	위암	
5	1485*	> 40	*	위암	다양한 질병이 혼재되어 안전
6	1485*	> 40	*	전립선염	
7	1485*	> 40	*	고혈압	
8	1485*	> 40	*	고혈압	
2	1306*	≤ 40	*	전립선염	다양한 질병이 혼재되어 안전
3	1306*	≤ 40	*	고혈압	
11	1306*	≤ 40	*	위암	
12	1306*	≤ 40	*	위암	

t–근접성(t–closeness) : 값의 의미를 고려하는 프라이버시 모델

- ℓ –다양성의 취약점*(쏠림 공격, 유사성 공격)을 보완하기 위해 모델

* ℓ –다양성의 취약점

- **쏠림 공격 (skewness attack)**
  - 정보가 특정한 값에 쏠려 있을 경우 ℓ –다양성 모델이 프라이버시를 보호하지 못함

〈쏠림 공격의 예〉
- 임의의 '동질 집합'이 99개의 '위암 양성' 레코드와 1개의 '위암 음성' 레코드로 구성되어 있다 가정
- 공격자는 공격 대상이 99%의 확률로 '위암 양성'이라는 것을 알 수 있음

• **유사성 공격 (similarity attack)**

– 비식별 조치된 레코드의 정보가 서로 비슷하다면 ℓ –다양성 모델을 통해 비식별 된다 할지라도 프라이버시가 노출될 수 있음

〈유사성 공격의 예〉

• 〈표 5〉는 3–다양성(ℓ =3) 모델을 통해 비식별 된 데이터

• 레코드 1,2,3이 속한 동질 집합의 병명이 서로 다르지만 의미가 서로 유사함(위궤양, 급성 위염, 만성 위염)

• 공격자는 공격 대상의 질병이 '위'에 관련된 것이라는 사실을 알아낼 수 있음

• 또 다른 민감한 정보인 급여에 대해서도 공격 대상이 다른 사람에 비해 상대적으로 낮은 급여 값을 가짐을 쉽게 알아낼 수 있음(30 ~ 50백만원)

○ (정의) 동질 집합에서 특정 정보의 분포와 전체 데이터 집합에서 정보의 분포가 t이하의 차이를 보여야 함

– 각 동질 집합에서 '특정 정보의 분포'가 전체 데이터집합의 분포와 비교하여 너무 특이하지 않도록 함

– 〈표 5〉에서 전체적인 급여 값의 분포는 30 ~ 110이나 레코드 1, 2, 3이 속한 동질 집합에서는 30 ~ 50으로 이는 전체 급여 값의 분포(30 ~ 110)와 비교할 때 상대적으로 유사한 수준이라 볼 수 있음

→ 공격자는 근사적인 급여 값을 추론할 수 있음

– t–근접성 모델은 이러한 동질 집합과 전체 데이터 집합 사이의 분포의 과도한 차이를 ℓ –다양성 모델의 취약점으로 규정함

● 〈표 5〉 ℓ –다양성 모델에 의해 비식별되었지만 유사성 공격에 취약한 사례 ●

구 분	속성자		민감한 정보		비고
	지역 코드	연령	급여(백만원)	질병	
1	476**	2*	30	위궤양	모두가 '위'와 관련한 유사 질병으로 취약
2	476**	2*	40	급성 위염	
3	476**	2*	50	만성 위염	
4	4790*	≥ 40	60	급성 위염	다양한 질병이 혼재되어 안전
5	4790*	≥ 40	110	감기	
6	4790*	≥ 40	80	기관지염	
7	476**	3*	70	기관지염	다양한 질병이 혼재되어 안전
8	476**	3*	90	폐렴	
9	476**	3*	100	만성 위염	

○ '정보의 분포'를 조정하여 정보가 특정 값으로 쏠리거나 유사한 값들이 뭉치는 경우를 방지

– 〈표 6〉에서 t-근접성 모델에 따라 레코드 1, 3, 8은 하나의 동질 집합

– 이 경우, 레코드 1, 3, 8의 급여의 분포는 (30 ~ 90)으로 전체적인 급여의 분포(30 ~ 110)와 큰 차이가 나지 않음

– 또한, 레코드 1, 3, 8의 질병 분포는 위궤양, 만성위염, 폐렴으로 병명이 서로 다르고 질병이 '위'와 관련된 것 이외에 '폐'와 관계된 것도 있어 특정 부위의 질병임을 유추하기 어려움

– 따라서 〈표 5〉의 경우와 비교하여 공격자가 공격 대상의 정보를 추론하기가 더욱 어려워짐

● 〈표 6〉 t-근접성 모델에 의해 비식별 조치된 데이터 사례 ●

구 분	속성자		민감한 정보		비고
	지역 코드	연령	급여(백만원)	질병	
1	4767*	≤ 40	30	위궤양	급여의 분포와
3	4767*	≤ 40	50	만성 위염	다양한 질병
8	4767*	≤ 40	90	폐렴	으로 안전
4	4790*	≥ 40	60	급성 위염	급여의 분포와
5	4790*	≥ 40	110	감기	다양한 질병
6	4790*	≥ 40	80	기관지염	으로 안전
2	4760*	3*	40	급성 위염	급여의 분포와
7	4760*	3*	70	기관지염	다양한 질병
9	4760*	3*	100	만성 위염	으로 안전

○ t수치가 0에 가까울수록 전체 데이터의 분포와 특정 데이터 구간의 분포 유사성이 강해지기 때문에 그 익명성의 방어가 더 강해지는 경향

– 익명성 강화를 위해 특정 데이터들을 재배치해도 전체 속성자들의 값 자체에는 변화가 없기 때문에 일반적인 경우에 정보 손실의 문제는 크지 않음

참고 4 비식별 조치 적정성 평가단 세부 평가수행 방법

사전 검토

- 평가 수행기관에서 제출한 기초자료와 인터뷰 등을 통해 평가대상 데이터에 개인 식별요소(식별자, 속성자) 포함 여부, 데이터 이용 목적, 적용된 비식별 조치 기법 등 검토
- 첫째, 평가 수행기관에서 작성 · 제출한 기초자료가 필수사항을 모두 포함하고 있고, 적절히 작성되었는지 검토
  - 기초자료가 충분하지 않은 경우 평가수행기관에 추가적인 자료 제출 및 보완을 요구
- 둘째, 평가 대상 데이터의 특성에 대해 확인하고 개인을 식별할 수 있는 식별 요소를 포함하고 있는지 확인
  - 평가 대상 데이터의 생성 및 관리되는 환경, 데이터의 크기, 시간 흐름에 따른 축적 여부 등 데이터의 특성에 대해 확인
  - 평가 대상 데이터의 식별자 또는 속성자에 식별요소를 포함하고 있는지 검토
  - 평가 대상 데이터가 개인 식별요소를 포함하고 있는 경우 개인 식별요소 제거 조치가 '부적정' 한 것으로 판단하고 비식별 조치 보강 요청
- 셋째, 기초자료로 제출된 '비식별 조치에 적용한 기법 · 세부기술'에 따라 비식별 조치가 적절히 수행되었는지 검토
  - '데이터 원본 예시', '비식별 조치된 평가 대상 데이터 셋 및 세부 항목별 명세', '비식별 조치에 적용한 기법 · 세부기술' 등 검토
  - '비식별 조치에 적용한 기법 · 세부기술'에 따라 개인 식별요소 제거 조치가 충분히 되지 않은 경우 '부적정' 한 것으로 판단하고 비식별 조치 보강 요청

재식별 시도 가능성 분석

- 데이터를 이용 또는 제공받는 자의 개인정보 재식별 의도와 능력, 개인정보 보호 수준 등을 통해 재식별 시도 가능성을 분석

1) 재식별 의도 및 능력 분석

- 데이터 이용자 또는 요청자의 재식별 의도 및 능력에 대한 검토 실시
- 평가단은 〈표 1〉 평가지표의 세부 질문에 대해 평가하고 개별 평가 지표별로 '예' 또는 '아니오'로 평가를 실시

● 〈표 1〉 재식별 의도 및 능력 분석 평가 지표 ●

구 분	세부 지표	평가
재식별 의도	• 데이터 이용자 또는 요청자가 데이터 제공자와 기존에 함께 업무를 수행하면서 상호 신뢰관계를 구축한 경험이 없음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터를 재식별 하는 경우 경제적인 이익이 있음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터를 재식별 하는 경우 비경제적인 이익이 있음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터를 제3의 이용자에게 사전 허가 없이 제공할 가능성이 있음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터 이용(제공) 관련 계약서에 재식별 금지 및 제3자에게 데이터 제공 제한 등의 문구를 반영하고 있지 않음	예/아니오
재식별 능력	• 데이터 이용자 또는 요청자가 개인정보 재식별을 시도 할 수 있는 전문 지식을 보유하고 있음	예/아니오
	• 데이터 이용자 또는 요청자가 개인정보 재식별을 시도 할 수 있는 재원(자금)을 보유 또는 조달할 수 있음	예/아니오
	• 데이터 이용자 또는 요청자가 개인정보 재식별을 위해 연계할 수 있는 다른 데이터베이스를 직접 보유하고 있거나 접근 할 수 있음	예/아니오
외부 정보 연계 가능성	• 인터넷, SNS 등에 평가대상 데이터와 결합 가능한 데이터가 존재할 수 있음	예/아니오

- 평가점수는 개인별로 각 평가지표에 대해 '예'로 평가한 지표의 개수를 합산해서 산출 (개인별 점수는 최대 9점, 점수가 높을수록 재식별 의도 및 능력이 큼)
- 개인별 점수를 합산한 후 전체 평가인원의 수로 나누어 '재식별 의도 및 능력 분석'의 평가 점수를 구하고, 〈표 2〉 평가 기준표에 따라 '높음', '중간', '낮음'으로 1차 평가결과 도출
- 1차 평가결과는 평가단 토의를 거쳐 확정하되, 1차 평가결과를 기준표와 달리 적용하는 경우에는 이에 대한 사유를 명확히 문서로 남겨야 함

● 〈표 2〉 재식별 의도 및 능력 분석 평가 기준표 ●

구 분	평가 기준
높음	• 평균 점수가 5점 이상인 경우
중간	• 평균 점수가 3점 이상, 5점 미만인 경우
낮음	• 평균 점수가 3점 미만인 경우

2) 개인정보 보호 수준 분석

- 데이터 이용자 또는 요청자의 개인정보 보호 수준을 검토하고 평가 실시
- 평가단 개인별로 〈표 3〉 평가 지표의 세부 질문에 대해 검토하고 개별 평가 지표별로 '예' 또는 '아니오'로 평가를 실시

〈표 3〉 개인정보 보호 수준 평가 지표

구 분	세부 지표	평가
개인정보 보호 능력	• 데이터에 접근할 수 있는 인력에 대해 보안각서를 받고 있음	예/아니오
	• 데이터에 접근할 수 있는 인력에 대해 정기적으로 보안 교육을 실시하고 있음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터의 보관 및 처리를 위한 관리계획을 수립하고 있음	예/아니오
	• 데이터 이용자 또는 요청자가 데이터의 보관 및 처리를 위한 관리계획에 따라 운영하고 있음	예/아니오
	• 데이터는 물리적, 기술적 보호 조치가 마련된 안전한 방법을 이용해서 제공하고 제공 받음	예/아니오
	• 침입차단 및 침입탐지 시스템이 설치된 서버, PC 등에서 이용됨	예/아니오
	• 데이터에 접근할 수 있는 인력의 접근권한 부여 및 접근 이력이 관리되고 있음	예/아니오
	• 데이터 이용자 또는 요청자가 보안 관리부서로부터 정기적으로 보안 점검을 받고 있음	예/아니오
	• 데이터 이용자 또는 요청자가 ISO27001, ISMS, PIMS 등의 인증을 받음	예/아니오

- 평가점수는 개인별로 각 평가지표에 대해 '예'로 평가한 지표의 개수를 합산해서 산출 (개인별 점수는 최대 9점, 점수가 높을수록 보호수준이 높음)
- 개인별 점수를 합산한 후 전체 평가인원의 수로 나누어 '개인정보 보호 수준'의 평균 점수를 구하고, 〈표 4〉 평가 기준에 따라 '높음', '중간', '낮음', '없음'으로 1차 평가결과를 도출
- 1차 평가결과는 평가단 토의를 거쳐 확정하되, 1차 평가결과를 기준표와 달리 적용하는 경우에는 이에 대한 사유를 명확히 문서로 남겨야 함

〈표 4〉 개인정보 보호 수준 분석 평가 기준표

구 분	평가 기준
높음	• 평균 점수가 6점 이상인 경우
중간	• 평균 점수가 4점 이상, 5점 미만인 경우
낮음	• 평균 점수가 4점 미만인 경우
없음	• 인터넷 등 일반에 공개하는 경우

3) 재식별 시도 가능성 분석

- '1) 재식별 의도 및 능력 분석', '2) 개인정보 보호 수준 분석'의 결과를 고려해서 비식별 조치된 데이터에 대한 재식별 시도 가능성을 평가
- 재식별 시도 가능성에 대한 평가는 '빈번한', '가능한', '가끔', '거의 없는' 등 4단계로 평가
- 아래 그림과 같이 '1) 재식별 의도 및 능력 분석'의 결과 값과, '2) 개인정보 보호 수준 분석'의 결과 값이 교차하는 지점의 평가값으로 재식별 시도 가능성 분석

● 재식별 시도 가능성 분석표 ●

2)개인정보 보호 수준				
없음	빈번한	빈번한	빈번한	
낮음	가능한	가능한	빈번한	
중간	가끔	가끔	가능한	
높음	거의 없는	거의 없는	가끔	
	낮음	중간	높음	1) 재식별 의도 및 능력

재식별 시 영향 분석

- 데이터가 의도적 또는 비의도적으로 재식별 되었을 때 정보주체에게 미치는 영향에 대해 분석
  - 특히, 경제적 피해 또는 비경제적인 피해(개인정보 또는 프라이버시 침해)를 줄 수 있는 가능성에 대해 평가를 실시
- 평가단 개인별로 〈표 5〉 평가지표 세부 질문에 대해 검토하고 지표별로 '예' 또는 '아니오'로 평가를 실시함
- 평가점수는 개인별로 각 평가지표에 대해 '예'로 평가한 지표의 개수를 합산해서 산출함(개인별 점수는 최대 4점, 점수가 높을수록 재식별시 영향이 큼)
- 개인별 점수를 합산한 후 전체 평가인원의 수로 나누어 '재식별시 영향 분석'의 평균 점수를 구하고, 〈표 6〉 평가 기준에 따라 '높음', '중간', '낮음'으로 1차 평가결과를 도출함

○ 1차 평가결과는 평가단 토의를 거쳐 확정하되, 1차 평가결과를 기준표와 달리 적용하는 경우에는 이에 대한 사유를 명확히 문서로 남겨야 함

● 〈표 5〉 재식별시 영향 분석 평가 지표 ●

구 분	세부 지표	평가
재식별시 영향	• 데이터가 재식별되었을 때 법적, 도덕적, 기술적 이슈로 사회적인 혼란을 가져올 가능성이 있음	예/아니오
	• 데이터가 재식별되었을 때 관련 정보주체의 개인정보 또는 프라이버시를 침해할 수 있음	예/아니오
	• 데이터가 재식별되었을 때 관련 정보주체에게 경제적 또는 비경제적 손실을 발생시킬 수 있음	예/아니오
	• 데이터가 재식별되었을 때 데이터 이용자 또는 요청자에게 경제적 또는 비경제적 손실을 발생시킬 수 있음	예/아니오

● 〈표 6〉 재식별시 영향 분석 평가 기준표 ●

구 분	평가 기준
높음	• 평균 점수가 2점 이상인 경우
중간	• 평균 점수가 1점 이상, 2점 미만인 경우
낮음	• 평균 점수가 1점 미만인 경우

계량 분석

○ 평가 대상 데이터의 특성을 고려하여 평가 대상 데이터에 대한 비식별 수준을 분석할 수 있는 분석 기법을 선정하고 분석 값(예시:k=5) 도출

※ 평가단에서 데이터의 특성, 비식별 정도 등을 고려해서 분석 기법 선정

– 비식별 정도를 분석하기 위한 기법에는 k–익명성(k–anonymity), ℓ–다양성(ℓ–diversity), t–근접성(t–closeness) 등의 프라이버시 보호 모델이 있음

○ 분석결과는 '평가 기준값' 결정시 참고할 수 있으며, 필요시 재분석 할 수 있음

○ 평가 대상 데이터에 대한 비식별 정도에 대한 계량 분석은 평가단에서 직접 수행 하거나, 외부의 공신력 있는 전문기관에 의뢰하여 수행할 수 있음

평가 기준값 결정

- 평가단은 비식별 조치의 적정성을 평가하기 위하여 'k–익명성', ' ℓ – 다양성', 't–근접성' 값 등을 단독 또는 복수개 이상으로 설정할 수 있음

- 평가 기준 값 설정시 고려 사항
  - 평가 대상 데이터의 속성자 항목 수, 규모, 시간 흐름에 따른 누적 데이터 존재 여부 등의 데이터 특징
  - 기초자료
  - 사전검토 결과
  - 재식별 시도 가능성 분석 결과
  - 재식별시 영향 분석 결과
  - 계량 분석 결과

- 필요시 계량 분석을 재실시 할 수 있으며, 이때 분석 기준 등에 대해서도 재검토 및 설정할 수 있음

● 평가 기준 값 사례 *●

재식별시 영향				
침해위험 높음	k = 5 ℓ = 2	k = 10 ℓ = 3	k = 10 ℓ = 4	k = 20 ℓ = 5 t 〈 0.3
침해위험 중간	k = 3 ℓ = 2	k = 5 ℓ = 2	k = 10 ℓ = 3	k = 10 ℓ = 4
침해위험 낮음	k = 3 ℓ = 2	k = 5 ℓ = 2	k = 5 ℓ = 2	k = 10 ℓ = 3
	거의 없는	가끔	가능한	빈번한

재식별 시도 가능성

* 세부 검토 기준 값은 단순 사례이며, 실제 적용시 일반적인 기준 값으로 이용하는 것은 적정하지 않을 수 있음. 기준값에 대한 결정은 평가단의 검토 및 논의에 따라 적용 프라이버시 모델 및 기준을 정하여 사용해야 함

적정성 평가

- 평가단은 평가 기준 값 결정에서 도출된 평가 기준 값과 계량 분석에서 계산된 분석 값을 비교하여 비식별 조치에 대한 1차 평가 결과를 도출

- 최종적인 평가는 1차 평가결과를 기초로 평가단 토의를 거쳐 최종 확정하며, 1차 평가 결과와 다른 결과를 도출한 경우에는 이에 대한 근거와 사유를 명확히 문서로 남겨야 함

1) k-익명성 값을 이용한 비식별 적정성 평가

- 계량 분석에서 분석된 평가 대상 데이터의 k-익명성 분석값이 평가단에서 결정한 '평가 기준값' 보다 작은 경우에는 개인 식별요소 제거 조치가 '부적정'한 것으로 평가

- 계량 분석에서 분석된 평가 대상 데이터의 k-익명성 분석값이 평가단에서 결정한 '평가 기준값' 보다 크거나 같은 경우에는 개인 식별요소 제거 조치가 '적정'한 것으로 평가

● k-익명성 기반 적정성 평가 사례표 ●

k-익명성 값을 이용한 비식별 조치에 대한 적정성 평가	
계량분석의 k-익명성 값 < 평가 기준값(k-익명성 값)	계량분석의 k-익명성 값 >= 평가 기준값(k-익명성 값)
⇩	⇩
'부적정' (개인 식별요소 제거 조치 필요)	'적정' (개인 식별요소 제거 조치 불필요)

2) ℓ-다양성 값을 이용한 비식별 적정성 평가

- 계량분석에서 분석된 평가대상 데이터의 ℓ-다양성 분석값이 평가단에서 결정한 '평가 기준값(ℓ-다양성)' 보다 작은 경우에는 개인 식별요소의 제거 조치가 '부적정'한 것으로 평가

- '계량 분석'에서 분석된 평가 대상 데이터의 ℓ-다양성 분석 값이 평가단에서 결정한 '평가 기준값(ℓ-다양성)' 보다 크거나 같은 경우에는 개인 식별요소 제거 조치가 '적정'한 것으로 평가

● ℓ–다양성 기반 적정성 평가 사례표 ●

ℓ–다양성 값을 이용한 비식별 조치에 대한 적정성 평가	
계량분석의 ℓ–다양성 값 < 평가 기준값(ℓ–다양성)	계량분석의 ℓ–다양성 값 >= 평가 기준값(ℓ–다양성)
⇩	⇩
'부적정' (개인 식별요소 제거 조치 필요)	'적정' (개인 식별요소 제거 조치 불필요)

3) t–근접성 값을 이용한 비식별 적정성 평가

- 계량 분석에서 분석된 평가 대상 데이터의 t–근접성 분석 값이 평가단에서 결정한 '평가 기준값(t–근접성)' 보다 작은 경우에는 개인 식별요소 제거 조치가 '적정'한 것으로 평가
  - 통상 t–근접성 값의 범위는 0에서 1 사이의 소수이며, 0에 가까울수록 개인을 식별할 가능성이 적다는 것을 의미함

- 계량 분석에서 분석된 평가 대상 데이터의 t–근접성 분석 값이 평가단에서 결정한 '평가 기준값(t–근접성)' 보다 크거나 같은 경우에는 개인 식별요소 제거 조치가 '부적정'한 것으로 평가

● t–근접성 기반 적정성 평가 사례표 ●

t–근접성 값을 이용한 비식별 조치에 대한 적정성 평가	
계량분석의 t–근접성 값 >= 평가 기준 값(t–근접성)	계량분석의 t–근접성 값 < 평가 기준 값(t–근접성)
⇩	⇩
'부적정' (개인 식별요소 제거 조치 필요)	'적정' (개인 식별요소 제거 조치 불필요)

개인정보 비식별 조치 가이드라인

- 비식별 조치 기준 및 지원 · 관리체계 안내 -

부록 1

– 개인정보의 범위 명확화 및 비식별 정보의 안전한 활용을 위한 –

개인정보 보호 관련 법령 통합 해설서

1 개인정보의 범위

개인정보보호법 제2조제1호

“개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제2조제1항제6호

“개인정보”란 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

신용정보의 이용 및 보호에 관한 법률 제2조제1호 및 제2호, 제34조제1항

“신용정보”란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 정보로서 다음 각 목의 정보를 말한다.

가. 특정 신용정보주체를 식별할 수 있는 정보
나. 신용정보주체의 거래내용을 판단할 수 있는 정보
다. 신용정보주체의 신용도를 판단할 수 있는 정보
라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보
마. 그 밖에 가목부터 라목까지와 유사한 정보

“개인신용정보”란 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보를 말한다.

“개인식별정보”란 생존하는 개인의 성명, 주소 및 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 국내거소신고번호 및 성별, 국적 등 개인을 식별할 수 있는 정보를 말한다.

1 개인정보의 개념

- 「개인정보 보호법」과 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)」에서는 개인정보의 개념을 규정하고 있으며, 「신용정보의 이용 및 보호에 관한 법률(이하 신용정보법)」에서는 개인신용정보와 개인식별정보의 개념에 대해 규정하고 있습니다.

○ 우선, 개인정보 보호법과 정보통신망법에서의 개인정보 개념 정의는 법률상 표현이 조금 다르게 되어 있으나, 법률 해석상 그 내용은 사실상 동일합니다.

- 두 법에서 정의하는 개인정보는 살아 있는 개인에 관한 정보로서 개인을 알아볼 수 있는 정보이며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보가 포함됩니다.
- 한편, 신용정보법 상의 개인신용정보 및 개인식별정보는 개인정보 보호법과 정보통신망법에서 말하는 개인정보 개념과 다르지 않습니다.

○ 현행 신용정보법은 개인신용정보를 "개인을 알아볼 수 있는 정보"일 것을 명시적으로 요구하지는 않지만, 개인을 알아볼 수 없는 신용정보가 개인신용정보에 포함되지 않는다고 보아야 합리적입니다.

○ 또한, 개인식별정보는 생존하는 개인의 성명, 주소 및 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 국내거소신고번호 등 개인을 식별할 수 있는 정보를 의미하기 때문입니다.

2 개인정보의 구체적 판단 기준

1 '생존하는' 개인에 관한 정보이여야 합니다.

가. **(법인의 정보)** 개인정보의 주체는 자연인이어야 하며, 법인 또는 단체의 정보는 개인정보에 해당하지 않습니다.

○ 따라서 법인 또는 단체의 이름, 소재지 주소, 대표 연락처(이메일 주소 또는 전화번호), 업무별 연락처, 영업실적 등은 개인정보에 해당하지 않습니다.

○ 그러나 법인 또는 단체의 정보에 해당하면서 동시에 개인에 관한 정보인 대표자를 포함한 임원진과 업무 담당자의 이름 · 주민등록번호 · 자택주소 및 개인 연락처, 사진 등은 개인정보에 해당합니다.

나. **(개인사업자에 관한 정보)** 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자등록번호, 매출액, 납세액 등은 사업체의 운영과 관련한 정보로서 원칙적으로 개인정보에 해당하지 않습니다.

○ 다만, 예외적으로 해당 정보가 사업자 개인의 직업 · 소득수준 · 활동영역 · 사회적 지위 등을 나타내는 정보로 이용되는 경우 개인정보로 보아야 하며, 개인사업자의 사업과 관련된 정보이면서 동시에 사업자 개인의 이름 · 주민등록번호 · 집주소 · 휴대전화번호 등은 개인정보에 해당합니다.

- 또한, 개인사업자의 고유식별정보 및 민감정보는 법령에 근거가 있거나 별도의 동의가 있어야 수집 · 이용이 가능하며, 고유식별정보 중 주민등록번호는 동의에 의하여서는 수집할 수 없으며 법령에 구체적인 근거가 있어야 처리할 수 있습니다.

다. **(사망자의 정보)** 개인정보 보호 법령상 개인정보는 '살아있는' 자연인에 관한 정보이므로 사망했거나 실종선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 개인정보로 볼 수 없습니다.

- 다만, 사망자의 정보라고 하더라도 유족과의 관계를 알 수 있는 정보는 유족의 개인정보에 해당합니다.

라. **(사물에 관한 정보)** 사람이 아닌 사물에 관한 정보는 원칙적으로 개인정보에 해당하지 않습니다. 그러나 해당 사물 등의 제조자 또는 소유자 등을 나타내는 정보는 개인정보에 해당합니다.

- 예를 들어, 특정 건물이나 아파트의 소유자가 자연인인 경우, 그 건물이나 아파트의 주소가 특정 소유자를 알아보는데 이용된다면 개인정보에 해당합니다.

2 '개인에 관한' 정보이여야 합니다.

가. **(개인에 관한 정보의 범위)** '개인에 관한 정보'란 당해 개인에 대한 사실 · 판단 · 평가 등 개인과 관련된 정보를 의미하므로, 특정 개인의 신원, 성격, 행위 등에 관한 것 또는 정보주체에 관한 평가 등에 영향을 미치는 것은 개인정보에 해당합니다.

나. **(2인 이상의 관련성)** '개인에 관한 정보'는 반드시 특정 1인만에 관한 정보이어야 한다는 의미가 아니며, 직 · 간접적으로 2인 이상에 관한 정보는 각자의 정보에 해당합니다.

- SNS에 단체 사진을 올린다면 사진의 영상정보는 사진에 있는 인물 모두의 개인정보에 해당하며, 의사가 특정 아동의 심리치료를 위해 진료 기록을 작성하면서 아동의 부모 행태 등을 포함하였다면 그 진료기록은 아동과 부모 모두의 개인정보에 해당합니다.

3 '정보'의 내용 · 형태 등은 제한이 없습니다.

가. **(정보의 내용 · 형태)** 정보의 내용 · 형태 등은 특별한 제한이 없어서 개인을 알아볼 수 있는 모든 정보가 개인정보가 될 수 있습니다.

- 즉, 디지털 형태나 수기 형태, 자동처리 정보와 수동처리정보 등 그 형태 또는 처리방식과 관계없이 모두 개인정보에 해당할 수 있습니다.

나. **(정보의 주관성 또는 객관성)** 정보주체와 관련되어 있으면 키, 나이, 몸무게 등 '객관적 사실'에 관한 정보나 그 사람에 대한 제3자의 의견 등 '주관적 평가' 정보 모두 개인정보가 될 수 있습니다.

- 또한, 그 정보가 반드시 '사실'이거나 '증명된 것'이 아닌 부정확한 정보 또는 허위의 정보라도 특정한 개인에 관한 정보이면 개인정보가 될 수 있습니다.

4 개인을 '알아볼 수 있는' 정보이여야 합니다.

- **('알아볼 수 있는'의 의미)**는 해당 정보를 '처리하는 자'의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당합니다.
- 여기서 '처리'란 개인정보 보호법 제2조제2호에 따른 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다.
- 현재 처리하는 자 외에도 제공 등에 따라 향후 처리가 예정된 자도 포함됩니다.
- 한편, 주민등록번호와 같은 고유식별정보는 해당 정보만으로도 정보주체인 개인을 알아볼 수 있지만, 생년월일의 경우에는 같은 날 태어난 사람이 여러 사람일 수 있으므로 다른 정보없이 생년월일 그 자체만으로는 개인을 알아볼 수 있다고 볼 수 없습니다.

5 다른 정보와 '쉽게 결합하여' 개인을 알아볼 수 있는 정보도 포함합니다.

- **('쉽게 결합하여'의 의미)**는 결합 대상이 될 정보의 '입수 가능성'이 있어야 하고 '결합 가능성'이 높아야 함을 의미합니다.
- '입수 가능성'의 의미는 두 종 이상의 정보를 결합하기 위해서는 결합에 필요한 정보에 합법적으로 접근 · 입수할 수 있어야 하며, 이는 해킹 등 불법적인 방법으로 취득한 정보까지 포함한다고 볼 수는 없습니다.
- '결합 가능성'의 의미는 합법적인 방법으로 정보를 입수하여도 현재의 기술 수준에 비추어 결합이 사실상 불가능하거나, 결합하는데 비합리적인 수준의 비용이나 노력이 수반된다면 이는 결합이 용이하다고 볼 수 없습니다.
- 따라서, 공유 · 공개될 가능성이 희박한 정보는 합법적 입수 가능성이 없다고 보아야 하며, 일반적으로 사업자가 구매하기 어려울 정도로 고가의 컴퓨터가 필요한 경우라면 '쉽게 결합'하기 어렵다고 보아야 합니다.

〈 참고 〉 폴란드 개인정보보호법

폴란드 개인정보보호법은 '식별을 위해서 불합리한 정도의 시간, 비용 및 인력을 필요로 하는 경우에는 식별을 가능하게 하는 정보로 간주해서는 안 된다'라고 하고 있음

3 개인정보의 개념 관련 판례 및 유권해석 사례

가. 판례(判例)

〈 판례 〉 휴대전화번호 뒤 4자리

대전지법 논산지원(2013고단17 판결)은 「휴대전화번호 뒷자리 4자」에 대하여, "휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더더욱 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를 식별하지 못한다 하더라도 그 뒷자리 번호 4자와 관련성이 있는 다른 정보(생일, 기념일, 집 전화번호, 가족 전화번호, 기존 통화내역 등)와 쉽게 결합하여 그 전화번호 사용자가 누구인지를 알아볼 수도 있다"고 하여 「개인정보보호법」 제2조제1호에 규정된 개인정보에 해당된다고 판시하고 있다.

나. 유권해석 사례

〈 개인정보보호위원회 결정 〉 배달음식점 고객의 전화번호 및 주소

개인정보보호위원회는 2012년 1월 30일 「개인정보 보호법 관련 법령해석 요청 건(의안 제2호)」에 대한 의결 이유에서 "배달음식점 고객의 전화번호 및 주소는 그 자체로는 특정 개인을 식별할 수 없지만, 용이하게 다른 정보와 결합하여 특정 개인을 식별할 수 있으므로, 「개인정보 보호법」 제2조제1호의 '개인정보'에 해당함"이라고 해석하고 있다. 용이하게 다른 정보와 결합하여 특정 개인을 식별할 수 있기만 하면 그 자체로서 특정 개인을 식별할 수 없는 경우에도 개인정보로 보고 있으므로, 의결 이유에서 지적한 '고객의 전화번호 및 주소'이외에도 개인정보로 인정할 수 있는 정보의 범위가 확장될 수 있다고 해석할 수 있다.

2 비식별 정보의 개념 및 재식별 시 제재

1 비식별 정보의 개념

가. **(비식별 정보의 개념)** 개인정보를 비식별 조치한 정보, 즉 '비식별 정보'란 정보의 집합물에 대해 「개인정보 비식별 조치 가이드라인」에 따라 적정하게 '비식별 조치'된 정보를 말합니다.

- '비식별 조치'란 정보의 집합물에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체 등의 방법을 통해 개인을 알아볼 수 없도록 하는 조치를 말합니다. (자세한 내용은 「개인정보 비식별 조치 가이드라인」 참고)
- 참고로 EU 개인정보지침은 'anonymization, 익명화'한 경우에는 지침이 적용되지 않도록 하고 있는데, 이 해설서에서 안내하는 '비식별 조치'는 EU의 익명화와 사실상 같은 개념입니다.
- 한편 비식별 정보가 개인정보에 해당하는지 여부가 의문이 있을 수 있으나, 가이드라인에 따라 적정하게 비식별 조치가 된 정보는 더 이상 특정 개인을 알아볼 수가 없으므로 개인정보가 아닌 것으로 추정됩니다.
- 개인정보가 아닌 것으로 추정된다는 의미는 개인정보에 해당한다는 반증이 없는 한 개인정보가 아니되, 개인정보라는 반증이 나오는 경우 개인정보로 본다는 뜻입니다.

나. **(비식별 정보의 활용)** 비식별 정보는 개인정보가 아닌 정보로 추정되므로 정보주체로부터의 별도 동의없이 해당 정보를 이용하거나 제3자에게 제공할 수 있습니다.

- 다만, 개인정보가 아닌 것으로 추정되더라도 불특정 다수에게 공개되는 경우에는 다른 정보를 보유하고 있는 누군가에 의해 해당 정보주체가 식별될 가능성이 있으므로 비식별 정보의 공개는 원칙적으로 금지됩니다.

다. **(비식별 정보의 보호)** 비식별 정보는 개인정보가 아닌 것으로 추정되지만, 새로운 결합 기술이 나타나거나 결합 가능한 정보가 증가하는 경우에는 정보주체가 '재식별'될 가능성이 있습니다. 따라서 비식별 정보라고 하더라도 필수적인 관리적 · 기술적 보호 조치는 이행해야 합니다. (자세한 내용은 「개인정보 비식별 조치 가이드라인」 참고)

2 재식별 시 제재

가. 비식별 정보를 재식별하여 이용하거나 제3자에게 제공한 경우에는 개인정보의 목적 외 이용 · 제공에 해당하여 5년 이하의 징역 또는 5천만원 이하의 벌금형에 처해집니다 (개인정보 보호법 제18조제1항 위반, 정보통신망법 제24조 및 제24조의2 위반, 신용정보법 제32조 및 제33조 위반)

※ 정보통신망법 적용 사업자는 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

- 예를 들어, 비식별 정보를 제3자에게 제공하면서 비식별 조치 요령을 공유하거나 공개되어 있는 알고리즘으로 암호화하여 쉽게 복호화될 수 있도록 정보를 제공하는 경우 등이 이에 해당 할 수 있습니다.

나. 비식별 정보를 처리하는 자(비식별 정보를 제공받은 자 포함)가 해당 정보를 이용하는 과정에서 재식별하게 된 경우에는 해당 정보를 즉시 처리중지하고 파기하여야 합니다.

- 추가적 비식별 조치없이 재식별된 정보를 보관하는 경우 5천만원 이하의 과태료가 부과됩니다 (개인정보 보호법 제15조 제1항 위반, 정보통신망법 제22조제1항 위반, 신용정보법 제15조 제2항 위반)

※ 정보통신망법 적용 사업자는 5년 이하 징역 또는 5천만원 이하 벌금형에 처해지며, 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음

〈 참고 〉 미국의 De-identified data

- 소비자 프라이버시 권리장전 Sec4.(2)에서는 'De-identified data'의 개념을 정의하고 해당 정보는 비개인정보로 취급

〈 참고 〉 EU의 개인정보 보호지침 서문 제26조

- EU 개인정보 보호지침의 서문 제26조에서는 정보주체의 신원을 확인할 수 없는 익명정보는 보호원칙이 적용되지 않음을 명시

〈 참고 〉 일본의 익명가공정보

● 개인정보 보호법에 빅데이터 활용 목적의 '익명가공정보'라는 개념을 신설

〈일본 개인정보 보호법 제2조제9항〉
이 법률에서 정하는 "익명가공정보"란 다음의 각 호에 해당하는 개인정보 구분에 대응하고 해당 각 호에 정하는 조치를 취하여 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻는 개인에 관한 정보로서, 해당 개인정보를 복원할 수 없도록 한 것을 말한다.

● 익명가공정보의 법적취급 : 복원불가능을 전제로 하여 정보주체의 동의를 받을 필요가 없고 제3자 제공도 자유로움, 다만 일정한 기술적 · 관리적 조치를 해야 함

● 개인정보취급사업자의 익명가공정보 작성시 의무사항

- 개인정보취급사업자가 익명가공정보를 작성할 때는 특정 개인을 식별하는 것 및 그 작성에 이용되는 개인정보를 복원할 수 없도록 가공해야 한다. (제36조 제1항)
- 개인정보취급사업자가 익명가공정보를 작성할 때는 정보의 누설을 방지하기 위하여 정보의 안전관리를 위한 조치를 하여야 한다. (제36조 제2항)

3 개인정보 보호법과 다른 법률과의 관계

1 일반 원칙

가. 일반법과 특별법이 저촉되면 특별법이 먼저 적용되고, 특별법에 규정이 없는 사항에 대해서는 일반법이 적용된다. (헌법재판소 2004. 9. 23. 2004헌가12 결정 참조)

나. 법률이 상호 모순, 저촉되는 경우에는 신법이 구법에, 그리고 특별법이 일반법에 우선하나, 법률이 상호 모순되는지 여부는 각 법률의 입법목적, 규정사항 및 그 적용범위 등을 종합적으로 검토하여 판단하여야 한다. (대법원 1989. 9. 12. 선고 88누6856 판결, 대법원 1995. 2. 3. 선고 94누2985 판결 등)

2 개인정보 보호법과 정보통신망법의 관계

가. 정보통신서비스 제공자에 대하여는 정보통신망법이 우선 적용되지만, 정보통신망법에 특별한 규정이 없고 개인정보 보호법과 상호 모순·충돌하지 않는 경우에는 개인정보 보호법이 적용됩니다.

나. 개인정보 보호법 제2조제1호의 개인정보 개념과 정보통신망법 제2조제6호의 개인정보 개념 정의는 개인정보의 예시와 관련하여 일부 차이가 있을 뿐 동일한 내용을 규정하고 있으므로 사실상 동일한 개념이라고 볼 수 있습니다.

○ 따라서, 개인정보의 개념과 개인정보가 아닌 것으로 추정되는 비식별 정보의 개념 또한 차이가 없습니다.

● **개인정보 보호법과 정보통신망법 상의 "개인정보" 정의 규정 비교** ●

「개인정보 보호법」 제2조제1호	정보통신망법 제2조제1항제6호
개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.	개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

3 개인정보 보호법과 신용정보법의 관계

가. 신용정보법 제3조의2는 "개인정보의 보호에 관하여 이 법에 특별한 규정이 있는 경우를 제외하고는 「개인정보 보호법」에서 정하는 바에 따른다"라고 하고 있으므로 신용정보법은 개인정보 보호법에 대해 특별법의 지위를 가집니다.

○ 따라서, 개인신용정보에 대해서는 신용정보법을 우선 적용하되, 신용정보법에 규정되어 있지 않는 사항은 개인정보 보호법을 적용하여야 합니다.

나. 신용정보법 상의 개인신용정보 및 개인식별정보는 금융거래 등에 사용되는 개인정보의 특수한 형태로 개인정보 보호법 상의 개인정보의 개념은 신용정보법 상의 개인신용정보 및 개인식별정보보다 포괄적인 개념입니다.

○ 따라서, 신용정보법 상의 개인신용정보와 개인식별정보는 당연히 개인정보 보호법 상의 개인정보에 해당한다고 봐야 하며, 개인정보 보호법 상 개인정보가 아닌 것으로 추정되는 비식별 정보는 신용정보법에서도 개인정보가 아닌 것으로 추정됩니다.

부록 2

질의 및 응답(Q&A)

부록 2 질의 및 응답(Q&A)

구분	질의 사항
주요개념 및 적용범위	❶ 개인정보 보호법과 정보통신망법, 신용정보법 등에서 규정하는 개인정보의 개념에 차이는 없는지?
	❷ 어떤 정보가 개인정보에 해당하는 지를 판단할 때 해당 정보를 처리하는 자의 관점에서 보아야 한다고 했는데, 이의 의미는?
	❸ 개인정보를 비식별 조치하는 경우 개인정보가 아닌 것으로 추정한다는데 이것의 법적 의미는?
	❹ 본 가이드라인이 통신 사업자나 금융기관 등에도 적용되는지?
	❺ 통계청 등 관련 법령에 따라 데이터를 수집, 연계 · 활용하는 기관들에 대해 본 가이드라인의 적용 여부는?
	❻ 개인정보 보호법 제18조제2항제4호에 따른 정보와 「개인정보 비식별 조치 가이드라인」에 따라 비식별 조치한 정보와의 차이는?
비식별 조치	❼ 본 가이드라인에서 말하는 비식별 조치는 무엇인가?
	❽ 고객정보를 제공받는 기관이 비식별 조치를 한다면, 제공하는 기관은 비식별 조치를 하지 않을 수 있는지?
	❾ 비식별 대상인 개인 식별정보의 구체적인 항목은 어떻게 되는지?
	❿ 비식별 조치가 적정한지 어떻게 알 수 있나?
	⓫ 평가단 구성 시 '데이터 이용 목적과 직접적인 이해관계가 없는 자'로 위원을 구성토록 하고 있음. 이 때, 평가단에 참여하는 내부전문가의 경우에는 이해관계자에 포섭될 수 있는데, 평가단 구성에 대한 구체적 기준은 무엇인지?
	⓬ 평가단이 단순히 k-익명성 값만을 가지고 판단할 가능성이 있는데?
	⓭ 적정성 평가 시 k-익명성을 기본으로 활용하되, 필요시 추가적인 평가모델(ℓ -다양성, t-근접성)을 활용하도록 규정하고 있는데, '필요시'에 대한 객관적인 기준은 무엇인지?
	⓮ 평가단이 '적정'으로 판단한 비식별 정보가 추후에 재식별된 경우 그 책임소재는?
비식별 정보 활용	⓯ 비식별 조치된 고객정보를 시장조사, 신상품 개발, 마케팅 전략수립 등에 활용하거나 제휴회사에 제공하고자 하는 경우 해당 고객의 동의가 필요한가?
	⓰ '적절한 수준으로 비식별 조치'된 데이터에 대해서는 제3자 제공 동의를 받지 않았더라도 다양한 비즈니스 목적으로 제3자에게 유상/무상으로 제공이 가능한지?
	⓱ 1대1 마케팅 등 맞춤형 서비스 목적으로 이용 가능한지?

비식별 정보 활용	⑱ 적절한 수준으로 비식별 조치'된 데이터에 대해서는 정보활용에 대한 동의를 받지 않았더라도 다양한 고객 분석, 신상품 기획, 세그먼트 마케팅 등의 목적에 활용할 수 있는가?
	⑲ 법령상 '민감정보'에 해당하는 건강정보 및 유전정보의 경우에도 비식별 조치를 한다면 개인의 동의없이 활용 가능한지?
	⑳ 유전정보도 다른 건강정보와 동일하게 취급해야 하는지 아니면 별도 강화된 조치가 필요한지?
	㉑ 고객 행태 분석을 위해 서비스 이용 기록이나 SNS 등에 공개된 정보를 수집하여 비식별 조치 후 이용하는 것이 가능한가?
	㉒ 해당 데이터를 가이드라인에 따라 적정성 평가를 받고 활용하다 새로운 분석을 위해 비식별 조치 방법을 변경하고자 할 때 이 경우 별도의 적정성 평가를 진행해야 하는지?
사후관리	㉓ 비식별 정보가 재식별되면 어떻게 해야 하나?
	㉔ 비식별 정보도 재식별 가능성이 있다고 하는데 비식별 조치가 제대로 안된 것이 아닌지?
	㉕ 제공한 비식별 정보의 모니터링 책임이 제공자에게 있는 것인지?
	㉖ '적절한 수준으로 비식별 조치'된 정보는 개인정보 보관기한 등과 무관하게 저장하여 활용할 수 있는지?
	㉗ 비식별 조치를 한 정보에 대한 열람, 정정 · 삭제 및 처리정지 등의 요구에 어떻게 대응해야 하는지?
	㉘ 개인이 재식별 된 경우, 개인정보 보호법 제34조의 '유출'로 보아 해당 정보주체에 대한 유출통지를 해야 하는지?
지원 및 관리체계 (재식별 법적 제재)	㉙ 다른 사업자가 보유한 DB를 결합하여 빅데이터 분석 등에 활용할 수 있는가?
	㉚ DB 결합을 위해 분야별 전문기관에 데이터를 제공하는 경우 식별자만을 제거하고 제3의 기관에서 제공한 알고리즘으로 임시대체키를 생성하여 붙인 뒤 다른 비식별 조치를 하지 않을 수 있는지?
	㉛ 업종별의 경우 전문기관이 서로 다른데 이업종의 DB결합시 각자 자신이 속한 업종의 전문기관의 지원을 받으면 되는 것인지?
	㉜ 이종 DB결합시 주민등록번호를 사용하여 임시 대체키를 만드는 것이 현행법 위반인지?
	㉝ 기업 내에서 서로 다른 부서간의 DB를 결합하여 이용하고자 하는 경우에도 반드시 외부의 전문기관을 통해야 하는지?
	㉞ 개인정보를 비식별 조치하여 활용할 경우 법적인 책임은 없는지?
	㉟ 가이드라인에서 정하는 대로 비식별 조치를 실시하였다고 가정할 때 의도하지 않은 재식별 발생시 면책이 가능한지?

주요개념 및 적용범위

문1 **개인정보 보호법과 정보통신망법, 신용정보법 등에서 규정하는 개인정보의 개념에 차이는 없는지?**

답 개인정보 보호법 제2조제1호의 개인정보 개념과 정보통신망법 제2조제1항제6호의 개인정보 개념은 일부 예시와 관련하여 차이가 있을 뿐 사실상 동일한 개념임
또한, 신용정보법 상의 개인신용정보와 개인식별정보는 금융거래 등에 사용되는 개인정보의 특수한 형태로 이는 개인정보 보호법 상의 개인정보에 해당함

문2 **어떤 정보가 개인정보에 해당하는 지를 판단할 때 해당 정보를 처리하는 자의 관점에서 보아야 한다고 했는데, 이의 의미는?**

답 개인정보 보호법 상 개인정보란 그 자체의 정보로 또는 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보를 의미하는 바, 여기서 '알아볼 수 있는'의 주체는 개인정보를 처리하는 자로 한정하여야 함
이는 만약 '알아볼 수 있는'의 주체를 불특정 제3자로 확대 해석하게 되면, 모든 정보가 다른 정보와 결합하여 개인정보가 될 수 있는 불합리한 결과가 초래되기 때문임
다만, '해당 정보를 처리하는 자'는 정보를 제공하는 관계에서는 해당 정보를 제공받은 자를 포함하는 개념임

문3 **개인정보를 비식별 조치하는 경우 개인정보가 아닌 것으로 추정한다는데 이것의 법적 의미는?**

답 본 가이드라인에 따라 특정 개인을 알아볼 수 없도록 비식별 조치가 적정하게 된 경우에는 개인정보에 해당한다는 반증이 없는 한 개인정보가 아닌 것으로 보되, 개인정보라는 반증이 나오는 경우 개인정보로 본다는 뜻임

문4 **본 가이드라인이 통신 사업자나 금융기관 등에도 적용되는지?**

답 본 가이드라인은 비식별 조치 기준과 지원 · 관리체계 등 비식별 정보를 안전하게 활용하기 위한 목적으로 행정자치부(개인정보 보호법), 방송통신위원회(정보통신망법), 금융위원회(신용정보법), 보건복지부(의료법) 등 관계부처와 공동으로 마련한 것으로 본 가이드라인은 통신 사업자나 금융기관 등 모든 사업자에 적용됨

문5 **통계청 등 관련 법령에 따라 데이터를 수집, 연계 · 활용하는 기관들에 대해 본 가이드라인의 적용 여부는?**

답 통계법 등 관련 개별 법령에서 정한 바에 따라 데이터를 수집, 연계 · 활용하는 기관들의 경우에는 본 가이드라인의 내용보다 관련 법령의 규정이 우선 적용되어야 함
따라서, 통계청 등이 관계 법령에 따라 통계작성 등 고유의 공공목적을 위해 데이터를 수집, 연계 · 활용하는 경우는 해당 법령에 근거한 비식별 조치 방식을 적용해야 함

문6 **개인정보 보호법 제18조제2항제4호에 따른 정보와 「개인정보 비식별 조치 가이드라인」에 따라 비식별 조치한 정보와의 차이는?**

답 개인정보 보호법 제18조제2항제4호에 따른 정보는 개인정보가 아닌 것으로 추정한다는 점에서는 비식별 정보와 동일하지만, 법에서 허용된 통계작성 및 학술연구 등을 위한 국한된 목적으로만 제공할 수 있다는 점에서 차이가 있어서 「개인정보 비식별 조치 가이드라인」에 따른 비식별 조치 중 적정성 평가는 제외할 수 있음

비식별 조치

문7 본 가이드라인에서 말하는 비식별 조치는 무엇인가?

답 "비식별 조치"란 정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소(식별자, 속성자)를 전부 또는 일부 삭제하거나 대체하는 등의 방법으로 개인을 알아볼 수 없도록 하는 조치를 말함

비식별 조치는 우선 '가명처리', '총계처리', '데이터 삭제', '데이터 범주화', '데이터 마스킹'과 같은 기법 등을 활용하여 개인을 알아볼 수 없도록 조치하고, 또 'k-익명성' 모델 등을 활용하여 비식별 조치가 적정한지 여부에 대한 평가절차를 거쳐야 함

문8 고객정보를 제공받는 기관이 비식별 조치를 한다면, 제공하는 기관은 비식별 조치를 하지 않을 수 있는지?

답 비식별 조치되지 않은 개인정보 제공은 개인정보 제3자 제공에 해당하므로 정보주체의 별도 동의가 없었다면 현행법 위반임

따라서, 정보주체로부터 제3자 제공에 대한 별도동의를 받지 않았다면 제공하는 기관이 비식별 조치를 한 후 제공하여야 함

문9 비식별 대상인 개인 식별정보의 구체적인 항목은 어떻게 되는지?

답 본 가이드라인에 따른 비식별 조치 대상은 정보집합물(데이터 셋)에 포함되어 있는 개인 식별요소(식별자 및 속성자)이며, 각 식별요소에 대한 비식별 조치 여부와 방법은 데이터 이용 목적 등을 고려하여 결정되어야 할 것임

식별자는 원칙적으로 삭제하여야 하고, 데이터 이용 목적상 반드시 필요한 식별자는 비식별 조치 후 활용하여야 함

속성자는 데이터 이용 목적과 관련이 없는 경우 삭제하고, 이용 목적과 관련이 있는 속성자 중 식별요소가 있는 경우에는 가명처리, 총계처리 등의 조치 기법을 활용하여 비식별 조치하여야 함

문10 비식별 조치가 적정한지 어떻게 알 수 있나?

답 비식별 조치가 적정한지에 대한 여부는 프라이버시 보호 모델인 'k-익명성' 등을 활용한 평가를 거쳐 결정됨

예를 들어, k값을 5로 정하여 비식별 조치하였다면 정보집합물 내에는 특정인을 식별할 수 있는 요소가 없음은 물론이고, 최소 5개 이상의 동일한 레코드(row, 列)가 존재하여 특정 개인을 식별하기 어려우므로 비식별 조치가 적정한 것으로 봄

문11 평가단 구성 시 '데이터 이용 목적과 직접적인 이해관계가 없는 자'로 위원을 구성토록 하고 있음. 이 때, 평가단에 참여하는 내부전문가의 경우에는 이해관계자에 포섭될 수 있는데, 평가단 구성에 대한 구체적 기준은 무엇인지?

답 평가단 구성에 내부 전문가를 참여시키고자 하는 경우에는 해당 데이터 이용 목적과 직접적인 이해관계가 없는 내부 전문가를 지정하여 평가 결과의 공정성과 신뢰성을 보장하여야 할 것이며, 이 경우 간접적인 이해관계자까지 모두 배재해야 할 필요는 없음

문12 평가단이 단순히 k-익명성 값만을 가지고 판단할 가능성이 있는데?

답 '비식별 적정성 평가단'이 단순히 k-익명성 값을 만족하는지 여부만을 평가하는 것이 아니라 평가대상 데이터의 특성, 재식별 시도 가능성 등을 고려하여 현재의 비식별 조치 수준이 적정한지, 재식별 위험이 없는지 여부 등을 종합적으로 평가하는 것임

문13 **적정성 평가 시 k-익명성을 기본으로 활용하되, 필요시 추가적인 평가모델(ℓ-다양성, t-근접성)을 활용하도록 하고 있는데, '필요시'에 대한 객관적인 기준은 무엇인지?**

답 본 가이드라인에 제시된 k-익명성을 활용한 평가는 최소한의 평가 수단이며, 평가 대상 데이터의 특성, 재식별 시도 가능성 등을 평가단에서 종합적으로 판단하여 추가적인 평가모델(ℓ-다양성, t-근접성)을 결정해야 함

예를 들어, k-익명성에 의해 범주화 되었더라도 각 레코드들이 충분한 다양성을 가지지 못하거나, 특정한 값에 쏠려 있다고 판단되는 경우에는 ℓ-다양성 또는 t-근접성을 추가적으로 적용해야 함

문14 **평가단이 '적정'으로 판단한 비식별 정보가 추후에 재식별된 경우 그 책임소재는?**

답 재식별에 대한 책임 소재는 당초 평가단의 평가 내용과 재식별된 경위 등을 종합적으로 고려하여 판단해야 할 사항임

당초 평가단 평가시 '적정'으로 판단할 만한 상당한 근거가 있었다면, 추후에 재식별 되었다는 이유만으로 책임을 부과하는 것은 곤란함

비식별 정보 활용

문15 **비식별 조치된 고객정보를 시장조사, 신상품개발, 마케팅 전략수립 등에 활용하거나 제휴회사에 제공하고자 하는 경우, 해당 고객의 동의가 필요한가?**

답 개인 식별요소 삭제 등 충분한 비식별 조치가 이루어졌다면 고객의 추가 동의 없이 시장조사, 신상품 개발, 마케팅전략 수립 등의 용도로 이용할 수 있음

다만, 제휴회사에 제공하는 경우에는 다른 정보와의 결합을 통한 재식별 가능성이 있으므로 재식별 위험관리 사항을 계약서에 반영하는 등 본 가이드라인에 따른 사항을 준수해야 할 것임

문16 **'적절한 수준으로 비식별 조치'된 데이터에 대해서는 제3자 제공 동의를 받지 않더라도 다양한 비즈니스 목적으로 제3자에게 유상/무상으로 제공이 가능한지?**

답 본 가이드라인에 따라 적정한 비식별 조치가 이루어졌다면 고객의 동의를 받지 않더라도 다양한 비즈니스 용도에 활용될 수 있도록 제3자에게 제공이 가능함. 이 경우 실비 수준의 수수료를 받고 비식별 정보를 제공할 수 있음

또한, 재식별 금지 및 재제공 제한, 재식별 위험시 통지 등의 내용을 해당 비식별 정보 제공과 관련한 계약서에 반드시 포함하여야 함

문17 **1대1 마케팅 등 맞춤형 서비스 목적으로 이용 가능한지?**

답 비식별 조치된 정보는 특정 개인을 알아볼 수 없으므로 1대1 마케팅 등 맞춤형 서비스 목적으로 활용하는 것이 현실적으로 불가능함

※ 개인 식별이 가능한 정보를 이용해 상품 판매 또는 홍보 등 1대1 마케팅을 하려면 현행 법령에 따라 정보주체의 사전 동의 필요

문18 **'적절한 수준으로 비식별 조치'된 데이터에 대해서는 정보활용에 대한 동의를 받지 않았더라도 다양한 고객 분석, 신상품 기획, 세그먼트 마케팅 등의 목적에 활용할 수 있는가?**

답 비식별 정보는 개인정보가 아닌 것으로 추정되는 바, 고객 분석, 신상품 기획, 세그먼트 마케팅 등의 목적으로 활용이 가능

다만, 세그먼트 마케팅을 위한 비식별 조치의 경우 특정 개인을 알아볼 수 없도록 세그먼트를 충분한 규모로 산정해야 함

문19 **법령상 '민감정보'에 해당하는 건강정보 및 유전정보의 경우에도 비식별 조치를 한다면 개인의 동의없이 활용 가능한지?**

답 개인정보 보호법상 민감정보에 해당하더라도 가이드라인에 따라 특정개인을 알아볼 수 없도록 비식별 조치한 경우 개인의 사전동의 없이 빅데이터 분석 등에 활용이 가능함
다만, 「생명윤리 및 안전에 관한 법률」에 근거한 인간 대상의 연구 목적으로 수집된 개인정보는 동 법 제18조에 의거 별도의 제공절차에 따라야 함

문20 **유전정보도 다른 건강정보와 동일하게 취급해야 하는지 아니면 별도의 강화된 조치가 필요한지?**

답 '유전정보'는 「디엔에이신원확인 정보의 이용 및 보호에 관한 법률」, 「생명윤리 및 안전에 관한 법률」에 따라 엄격히 보호되고 있는 정보이므로 해당 법률에서 정하는 별도의 강화된 조치가 필요함

문21 **고객 행태 분석을 위해 서비스 이용 기록*이나 SNS 등에 공개된 정보를 수집하여 비식별 조치 후 이용하는 것이 가능한가?**

*인터넷 접속정보, 웹사이트 방문정보, 사용하는 단말기 정보 등

답 합법적으로 수집한 정보라면 비식별 조치 후 이용하는 것은 가능하며, 이 경우 정보주체의 동의를 받지 않아도 됨

문22 해당 데이터를 가이드라인에 따라 적정성 평가를 받고 활용하다 새로운 분석을 위해 비식별 조치 방법을 변경하고자 할 때 이 경우 별도의 적정성 평가를 진행해야 하는지?

답 본 가이드라인에 따른 적정성 평가는 데이터 마스킹, 총계처리 등 비식별 기법이 적용된 정보를 대상으로 하여 비식별 조치가 적정하게 이루어졌는지 여부를 평가하는 것임
따라서, 당초 적용된 비식별 기법을 변경하여 다른 기법을 적용하는 경우에는 기존 평가 대상의 변경이 수반되므로 추가적인 적정성 평가가 진행되어야 함

사후관리

문23 비식별 정보가 재식별되면 어떻게 해야 하나?

답 사업자 등은 비식별 정보를 활용하는 과정에서 정기적인 모니터링과 필수적인 안전조치 등을 통해 재식별 위험을 최소화해야 함
다만, 비식별 정보의 처리 과정에서 비의도적으로 특정 개인을 재식별하게 된 경우에는 즉시 그 정보의 처리를 중단하고 파기조치를 하여야 함

문24 비식별 정보도 재식별 가능성이 있다고 하는데 비식별 조치가 제대로 안된 것이 아닌지?

답 재식별 가능성이 현저하다면 이는 비식별 조치가 제대로 이루어지지 않은 것임

※ 비식별 조치가 충분히 이루어졌다면 그 시점에서 재식별은 불가능

다만, 비식별 조치가 적정하게 된 경우에도 새로운 결합기술이 출현하고 입수가능한 정보가 증가하는 경우에는 사후에 재식별이 될 수 있음
따라서, 비식별 조치가 적정하게 된 경우에도 재식별 방지를 위해 필수적인 안전조치는 이행하여야 함

문25 제공한 비식별 정보의 모니터링 책임이 제공자에게 있는 것인지?

답 비식별 정보를 이용하거나 제3자에게 제공하려는 사업자 등은 해당 정보의 재식별 가능성을 정기적으로 모니터링 해야 함

이미 제공된 비식별 정보의 모니터링 책임은 과거에 그 정보를 제공한 자가 아니라 현재 그 정보를 이용하는 사업자 등에게 있음

문26 '적절한 수준으로 비식별 조치'된 정보는 개인정보 보관기한 등과 무관하게 저장하여 활용할 수 있는지?

답 비식별 정보는 개인정보가 아닌 것으로 추정되므로 보관 및 이용 목적 · 기간을 뚜렷하게 한 후 해당 목적 및 기간종료 시까지 저장하여 활용할 수 있음

다만, 비록 비식별 정보가 특정 개인을 알아볼 수는 없더라도, 재식별 의도가 있는 제3자가 부정한 목적으로 활용하지 않도록 필수적인 안전조치는 이행하여야 함

문27 비식별 조치를 한 정보에 대한 열람, 정정 · 삭제 및 처리정지 등의 요구에 어떻게 대응해야 하는지?

답 비식별 조치된 정보는 요구자에 대한 정보를 확인할 수 없으므로 개인정보 열람, 정정 · 삭제 및 처리정지 등이 현실적으로 불가능

문28 개인이 재식별 된 경우, 개인정보 보호법 제34조의 '유출'로 보아 해당 정보주체에 대한 유출통지를 해야 하는지?

답 '개인정보 유출'은 '법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우'를 의미하며, 정보처리 과정에서 우연히 개인이 재식별 되었다는 사실만으로는 개인정보 유출로 볼 수 없으므로 유출통지 대상이 아님

※ '개인정보처리자의 통제 상실' 및 '제3자의 접근 허용'에 해당하지 않음

다만, 재식별된 정보를 파기하지 않고 보관하다가 해커 등 권한 없는 제3자에게 그 정보가 노출되었다면 '개인정보 유출'에 해당하므로 지체없이(5일 이내, 정보통신망법 적용 사업자는 24시간 이내) 유출통지를 해야 할 것임

지원 및 관리체계

문29 다른 사업자가 보유한 DB를 결합하여 빅데이터 분석 등에 활용할 수 있는가?

답 정보주체의 동의없이 당사자간 개인정보를 직접 주고받는 것은 현행법 상 허용되지 않음
다만, DB 결합 과정에서만 임시로 매칭키 역할을 하는 '임시 대체키'를 부여하고 비식별 조치한 후 신뢰할 수 있는 전문기관이 결합하는 것은 가능

문30 DB 결합을 위해 분야별 전문기관에 데이터를 제공하는 경우 식별자만을 제거하고 제3의 기관에서 제공한 알고리즘으로 임시대체키를 생성하여 붙인 뒤 다른 비식별 조치를 하지 않을 수 있는지?

답 직접적인 식별자만 제거하고 속성자에 대한 비식별 조치 없이 분야별 전문기관에 데이터를 제공하는 행위는 본 가이드라인에 따른 충분한 비식별 조치가 아님
분야별 전문기관에 데이터 결합을 위해 제공하는 정보는 본 가이드라인에서 정하는 비식별 조치 및 '비식별 조치 적정성 평가단'의 평가를 거쳐 비식별 조치를 적정하게 한 후에 제공해야 함

문31 업종별의 경우 전문기관이 서로 다른데 이업종의 DB결합시 각자 자신이 속한 업종의 전문기관의 지원을 받으면 되는 것인지?

답 DB 결합을 지원할 전문기관을 선택하고자 하는 경우 ① 산업내 기업간 결합은 해당 분야 전문기관에서 결합을 지원하고, ② 이종산업간 결합은 대량의 정보집합물을 결합하고자 하는 기업이 속해 있는 분야별 전문기관에서 수행

※ 분야별 전문기관은 한국인터넷진흥원, 한국신용정보원, 금융보안원, 사회보장정보원, 한국정보화진흥원 중에서 소관부처가 공문으로 지정 · 공표하여 운영하고 필요시 추가 지정 가능

당해 산업을 지원해 주는 전문기관이 없는 경우에는 한국인터넷진흥원 또는 한국정보화진흥원에서 지원을 받으면 됨

문32 이종 DB결합 시 주민등록번호를 사용하여 임시 대체키를 만드는 것이 현행법 위반인지?

답 개인정보 보호법 제24조의2에 따라 주민등록번호는 법령에서 구체적으로 요구하거나 허용하는 경우 등을 제외하고는 처리가 엄격히 제한됨

따라서, 임시 대체키 생성 시 주민등록번호를 사용하는 것은 현행 법령에서 구체적으로 요구하거나 허용하는 경우 등으로 볼 수 없으므로 현행법 위반의 소지가 있음

문33 기업 내에서 서로 다른 부서간의 DB를 결합하여 이용하고자 하는 경우에도 반드시 외부의 전문기관을 통해야 하는지?

답 기업 내에서 서로 다른 부서간 DB를 결합하여 이용하고자 하는 경우에는 반드시 외부의 전문기관을 통할 필요는 없음

다만, 기업내 DB결합 시에도 결합 전 · 후 본 가이드라인에 따른 비식별 조치 및 적정성 평가를 수행하여야 하며, 결합과정에서 임시 대체키를 활용할 경우에는 결합대상 정보를 관리하지 않는 제3의 부서가 임시 대체키를 안전하게 생성 · 관리하고 재식별 시도 금지 및 재식별시 즉시 파기 등 필수 보호조치를 엄격히 해야 함

이 경우 평가단은 동일한 평가단에서 평가를 수행할 수 있음

문34 개인정보를 비식별 조치하여 활용할 경우 법적인 책임은 없는지?

답 본 가이드라인에 따라 특정 개인을 알아볼 수 없도록 비식별 조치하여 활용하는 경우에는 개인정보 보호법 상 목적 외 이용 · 제공 등에 관련한 책임은 없음. 다만, 적정한 비식별 조치 없이 활용하는 경우에는 책임이 있음

또한, 다른 정보와 결합하여 재식별 되지 않도록 필수적인 관리조치는 이행해야함. 즉, 비식별 정보에 대한 관리적 · 기술적 보호조치*와 재식별이 되는 경우 정보처리를 즉시 중단하고 파기 조치를 하는 등 가이드라인에서 정한 조치사항을 이행하지 않아 비식별 정보가 재식별이 되면 그에 따른 법적인 책임이 있음

* 비식별 정보파일에 대한 접근권한 관리 및 접근 통제, 비식별 정보파일 유출 시 대응계획 수립 등

문35 가이드라인에서 정하는 대로 비식별 조치*를 실시하였다고 가정할 때 의도하지 않은 재식별 발생 시 면책이 가능한지?

* 비식별 기법 적용 후 전문가 평가결과(k-익명성 등) '적정'인 경우

답 본 가이드라인에 따라 특정 개인을 알아볼 수 없도록 충분한 비식별 조치를 실시하였다면 고의성 없는 재식별 사실만으로 책임을 부과할 수는 없음

다만, 의도적으로 비식별 정보가 쉽게 재식별 될 수 있도록 이용 · 제공하거나, 재식별 정보를 보호조치 없이 보관 · 이용 · 제공한 경우에는 관련 법령에 따른 벌칙*이나 과태료**가 부과될 수 있음

* 재식별 정보 이용 · 제공시 : 5년 이하 징역 또는 5천만원 이하 벌금(정보통신망법 적용 사업자는 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음)

** 파기 조치 없이 보관 : 5천만원 이하 과태료(정보통신망법 적용 사업자는 5년 이하 징역 또는 5천만원 이하 벌금형 및 위반행위 관련 매출액의 3% 이하 과징금이 추가 부과될 수 있음)

본 가이드라인은 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부 등 관계부처가 합동으로 작성하였습니다.

각 부처가 개인정보 비식별 조치와 관련하여 기존에 발간한 지침, 안내서, 가이드라인 등은 2016. 6. 30일 부로 일괄 폐지되고 2016. 7. 1일 부터는 본 가이드라인이 적용됨을 알려드립니다.

개인정보 비식별 조치 가이드라인
-비식별 조치 기준 및 지원 · 관리체계 안내-

2016년 6월 28일 인쇄
2016년 6월 30일 발행

발행처 | 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부
제 작 | 호정씨앤피

개인정보 암호화 조치 안내서

(Ver 1.0)

2012. 10.

행정안전부 KISA 한국인터넷진흥원

본 안내서는 “개인정보 보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적 보호조치 중 “암호화”에 대한 안내를 위해 마련하였습니다.

본 안내서는 개인정보처리자가 주민등록번호의 저장·전송시 필요한 암호화 수행방식과 사례 등을 소개하고 있으며 수록된 암호화 알고리즘 등은 2012년 10월 기준으로 작성되었습니다.

따라서 본 안내서 이용시 암호화 알고리즘에 대한 최신 정보를 확인하시기 바랍니다. 또한 개인정보처리시스템별 환경에 따라 사례 등의 적용방식이 달라질 수 있음을 알려드립니다.

목 차

Ⅰ. 개요 ····· 1

제1절 목적 ····· 1
제2절 적용 대상 ····· 1
제3절 용어 정의 ····· 1

Ⅱ. 암호화 종류 및 제도 ····· 4

제1절 암호화의 필요성 ····· 4
제2절 암호화의 종류 및 특징 ····· 4
2.1 대칭키 암호화 ····· 4
2.2 공개키 암호화 ····· 5
2.3 일방향(해쉬함수) 암호화 ····· 6
제3절 안전한 암호 알고리즘 ····· 6
3.1 SEED ····· 7
3.2 ARIA-128/192/256 ····· 8
3.3 SHA-224/256/384/512 ····· 8
3.4 AES-128/192/256 ····· 8
3.5 Blowfish ····· 8
3.6 RSA ····· 9
3.7 Hash-DRBG ····· 9
제4절 암호화 관련 제도 ····· 10
4.1 개인정보 보호법 ····· 10
4.2 전자정부법 ····· 11
4.3 정보통신망 이용촉진 및 정보보호 등에 관한 법률 ····· 12
4.4 전자금융거래법, 전자금융감독규정 ····· 14

Ⅲ. 개인정보 암호화 방식 ····· 20

제1절 전송시 암호화 ····· 20
1.1 웹서버와 클라이언트 간 암호화 ····· 20
1.2 개인정보처리시스템 간 암호화 ····· 22
1.3 개인정보취급자 간 암호화 ····· 25

목 차

제2절 저장시 암호화 ····· 27
2.1 개인정보처리시스템 암호화 ····· 27
2.2 업무용 컴퓨터 암호화 ····· 35

Ⅳ. 개인정보 암호화 적용사례 ····· 38

제1절 전송시 암호화 ····· 38
1.1 웹서버와 클라이언트 간 암호화 사례 ····· 38
1.2 개인정보처리시스템 간 암호화 사례 ····· 38
1.3 개인정보취급자 간 암호화 사례 ····· 39

제2절 저장시 암호화 ····· 40
2.1 개인정보처리시스템 암호화 사례 ····· 40
2.2 업무용 컴퓨터 암호화 사례 ····· 44

Ⅴ. FAQ ····· 45

[붙임 1] 국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록 ····· 49

[붙임 2] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화) ····· 50

Ⅰ 개 요

제1절 목적

❍ 개인정보 보호법에서는 개인정보에 대한 안전성 확보조치 의무를 규정하고 있으며 그중 하나로 암호화 조치를 수행토록 하고 있다.

❍ 본 안내서는 개인정보처리자가 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송·수신하거나 저장하는 경우 암호화 기준을 제시하고 적용방법 및 적용사례 등의 안내를 목적으로 한다.

<관련 근거>

☞ 「개인정보 보호법」제24조(고유식별정보의 처리제한) 제3항 및 동법 시행령 제21조(고유식별정보의 안전성 확보조치)

☞ 「개인정보 보호법」제29조(안전조치의무) 및 동법 시행령 제30조(개인정보의 안전성 확보조치)

☞ 「개인정보 보호법」시행령 제30조(개인정보의 안전성 확보조치) 제3항에 따른 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2011-제43호) 제7조

제2절 적용 대상

❍ 개인정보 보호법에 따라 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 저장·전송하는 개인정보처리자를 대상으로 한다.

제3절 용어 정의

❍ "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

- “개인정보취급자”는 개인정보처리자의 지휘, 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
- “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- “개인정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
- “공공기관”이란 개인정보 보호법 제2조 및 동법시행령 제2조에 따른 국회, 법원, 헌법재판소, 중앙선관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체, 국가인권위원회, 공공기관의 운영에 관한 법률 제4조에 따른 공공기관, 지방공기업법에 따른 지방공사와 지방공단, 특별법에 따라 설립된 특수법인, 초·중등교육법, 고등교육법 및 그 밖의 다른 법률에 따라 설치된 각급 학교를 말한다.
- “내부망”이란 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
- “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 말한다.
- “보안서버”란 인터넷상에서 사용자 PC와 웹서버 사이에 송·수신되는 개인정보를 암호화하여 전송하는 서버를 말한다.
- “보조저장매체”라 함은 이동형 하드디스크(HDD), USB메모리, CD (Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.
- “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

❍ “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.

❍ “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

❍ “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

❍ “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

❍ “정보통신망”이란 ’전기통신기본법’ 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체계를 말한다.

Ⅱ 암호화 종류 및 제도

제1절 암호화의 필요성

- 정보통신 기술 발전에 따라 개인정보의 저장·유통이 대량화, 광역화, 네트워크화 되고 있어 이렇게 저장·유통되는 개인정보는 다양한 위협에 쉽게 노출되고 있다.
- 공격자는 정보통신망을 통해 개인정보 송수신시 패킷 도청 소프트웨어를 사용하여 가로채거나 또는 개인정보가 저장된 서버의 취약점을 찾아 고유식별정보 등과 같은 중요한 개인정보를 해킹하게 된다. 이러한 위협으로부터 중요 정보를 보호하기 위해서 개인정보의 전송 및 저장시 암호화가 필요하다.
- 암호화란 일상적인 문자로 쓰인 평문을 암호키를 소유하지 않은 사람이 알아볼 수 없도록 기호 또는 다른 문자 등의 암호문으로 변환하는 방법으로 정보의 기밀성 및 무결성, 사용자 인증 등을 위해 광범위하게 이용하고 있다.
- 최근 사회 전 분야에 걸쳐 개인정보 유출사고의 지속적인 발생으로 인해 제정된 개인정보보호법에 개인정보에 대한 안전성을 확보하기 위한 조치의무를 규정하고 있으며 전송 또는 저장 정보의 암호화 조치는 선택이 아닌 반드시 수행해야 할 항목으로서 위치하고 있다.

제2절 암호화 종류 및 특징

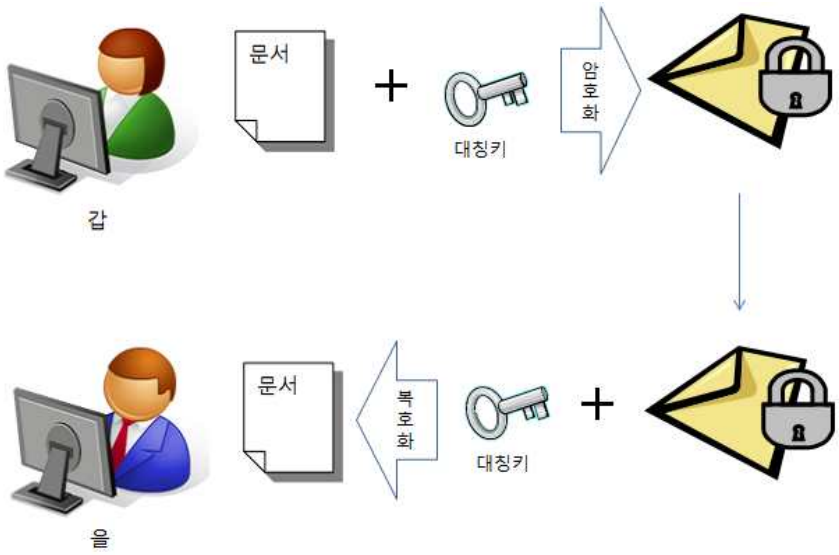
2.1 대칭키 암호화

- 대칭키 암호화 방식은 전송하고자 하는 평문을 암호화하고 복호화하는데 동일한 키를 사용하는 방식이다.
- 대칭키 암호화 방식은 공개키 암호화 방식에 비해 빠른 처리속도를 제공하고, 암호키의 길이가 공개키 암호화 방식보다 상대적으로 작아서 일반적인 정보의 기밀성을 보장하기 위한 용도로 사용되고 있다.

❍ 반면에 정보 교환 당사자 간에 동일한 키를 공유해야 하므로 여러 사람과의 정보 교환 시 많은 키를 유지 및 관리해야 하는 어려움이 있다.

❍ 대표적인 대칭키 암호 알고리즘은 국내의 SEED, ARIA, 미국의 DES, Triple-DES, AES, 유럽의 IDEA, 일본의 FEAL, MISTY 등이 있다.

❍ 대칭키 암호화 방식의 기본 개념은 <그림 1>과 같다.



<그림 1 > 대칭키 암호화 방식

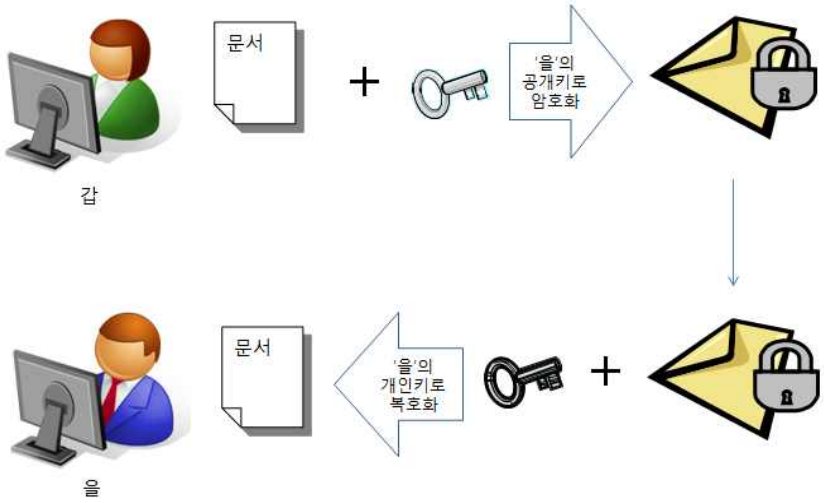
2.2 공개키 암호화

❍ 공개키 암호화 방식은 공개키와 개인키의 키 쌍이 존재하여 평문을 암·복호화하는데 서로 다른 키를 사용하는 방식으로 비대칭키 암호화 방식이라고도 불린다,

❍ 공개키 암호화 방식은 데이터 암호화 속도가 대칭키 암호화 방식에 비해 느리기 때문에 일반적으로 대칭키 암호화 방식의 키 분배나 전자서명 또는 카드번호와 같은 작은 크기의 데이터 암호화에 많이 사용되고 있다.

❍ 대표적인 공개키 암호 알고리즘으로는 국내에는 KCDSA가 있으며 국외에서는 RSA, ElGamal, ECC 등이 있다.

❍ 공개키 암호화 방식의 기본 개념은 <그림 2>와 같다.



<그림 2> 공개키 암호화 방식

2.3 일방향(해쉬함수) 암호화

❍ 일방향 암호화 방식은 해쉬함수를 이용하여 암호화된 값을 생성하며 복호화 되지 않는 방식이다.

❍ 해쉬함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해쉬값만으로 입력 메시지를 유추할 수 없어 전자서명 체계와 함께 데이터의 무결성을 위해 사용된다. 비밀번호와 같이 복호화가 필요 없지만 입력 값의 정확성 검증이 필요한 경우에 사용하고 있다.

❍ 대표적인 해쉬함수로는 SHA-2(SHA-224/256/384/512), RIPEMD-160 등과 국내에서 개발한 HAS-160이 있다.

제3절 안전한 암호 알고리즘

❍ 개인정보의 안전성 확보조치 기준 제7조제6항의 '안전한 암호알고리즘(이하 '암호알고리즘'이라 한다)'이란 국내외 전문기관에서 권고하는 알고리즘을 의미한다.

❍ 국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)의 권고를 중심으로 구성하고 있으며 이에 따른 암호 알고리즘은 [표 1]과 같다.

[표 1] 안전한 암호 알고리즘(예시)

구분	알고리즘 명칭
대칭키 암호 알고리즘	SEED ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512 Whirlpool 등

※ 공공기관은 "[붙임 1] 국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록"을 참고

- 본 안내서에서 권고하는 암호 알고리즘 등은 2012년 10월 기준으로 작성됨에 따라 국내외 암호전문기관의 최신 정보를 반드시 확인하도록 한다.

3.1 SEED

❍ SEED는 순수 국내기술로 개발한 대칭키 암호 알고리즘으로 128/256 비트 키를 지원하며, 128 비트 지원의 경우 1999년 정보통신단체표준(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/IEC와 IETF의 블록 암호 알고리즘 표준으로 제정되었다.

3.2 ARIA-128/192/256

❍ ARIA는 대칭키 방식의 국가 암호화 알고리즘으로 128 비트 블록 단위로 데이터의 암호화, 복호화를 수행하는 블록 암호 알고리즘이다. 128/192/256 비트 키를 지원하며 2004년에 한국산업규격 KS 표준으로 제정되었다.

3.3 SHA-224/256/384/512

❍ SHA는 해쉬함수로서 1993년 미국 표준기술연구소(NIST)에서 해쉬함수의 표준으로 개발한 SHA-1에 보안 취약점의 존재 가능성이 제기됨에 따라 SHA-2라는 명칭으로 해쉬값의 크기가 224/256/384/512 비트를 가지는 SHA-224/256/384/512의 해쉬함수가 표준화 되었다.

3.4 AES-128/192/256

❍ AES는 미국 표준기술연구소(NIST)에서 연방 정보처리 표준으로 발표한 대칭키 암호 알고리즘으로 128 비트의 블록크기를 가지며 키 길이는 128/192/256 비트를 가진다. 키 길이가 가변적이고 라운드 수도 블록 크기에 따라 가변적인 알고리즘으로 안전성과 성능의 요구에 따라 유연하게 사용이 가능하다.

3.5 Blowfish

❍ 1993년 개발한 대칭키 암호 알고리즘으로 가변적인 키 길이(32~448 비트)를 가지며, 구현이 간단하고 알고리즘의 안전성을 분석하기 쉬우며, 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용이 가능하다.

3.6 RSA

❍ RSA는 1983년에 미국 매사추세츠 공과대학교(MIT)에서 개발한 공개키 암호 알고리즘의 하나로 소인수분해의 어려움에 안전성의 기반을 두고 있으며, 대칭키 암호 알고리즘과 달리 메시지 암호화 등에 사용할 수 있도록 상대방에게 공개하는 공개키와 공개키로 암호화된 메시지를 복호화하는데 사용되는 비밀키를 사용한다. RSA 알고리즘을 활용한 암호시스템은 대칭키의 안전한 분배 및 관리문제를 해결하기 위해 널리 이용되며, 메시지 암·복호화, 전자서명 등에 사용된다.

3.7 Hash_DRBG

❍ Hash_DRBG는 해쉬함수를 이용하여 의사난수를 생성하는 난수발생기이다. 난수는 암호학적으로 대칭키 암호 알고리즘의 비밀키, 스트림암호 알고리즘의 초기화벡터, 공개키 암호 알고리즘 RSA의 큰 소수 등을 생성할 때 사용되는 것으로 난수를 생성하는 과정의 안전성에 결함이 있다면 이는 암호 알고리즘 자체의 안전성에 영향을 미치게 된다. Hash_DRBG는 이러한 난수를 해쉬함수를 이용해 안전하게 생성하는 난수발생기이며 HAS-160, SHA-2 등의 해쉬함수를 사용할 수 있다.

제4절 암호화 관련 제도

4.1 개인정보 보호법

4.1.1 적용 대상

❍ 공공기관, 법인, 단체 및 개인을 포함한 모든 개인정보처리자를 적용 대상으로 한다.

4.1.2 암호화 관련 주요 내용

❍ 개인정보 보호법 제24조 제3항

> **제24조(고유식별정보의 처리 제한)**
> ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 **대통령령**으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

❍ 개인정보 보호법 제29조

> **제29조(안전조치의무)**
> 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 **대통령령**으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

❍ 개인정보 보호법 시행령 제30조 제1항 제3호 및 제3항

> **제30조(개인정보의 안전성 확보 조치)**
> ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
> 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
> ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다.

❍ 개인정보 보호법 시행령 제30조 제3항에 따른 '개인정보의 안전성 확보조치 기준 제7조'(행정안전부고시 제2011-제43호)

※ 세부 설명은 '[붙임 2] 개인정보 보호법 암호화 관련 세부 내용' 참조

• 개인정보 위험도 분석기준 및 해설서(행정안전부 공고 제2012-112)는 www.privacy.go.kr에서 다운로드 받을 수 있다.

4.2 전자정부법

4.2.1 적용 대상

❍ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 소속기관, 지방자치단체 및 공공기관을 대상으로 한다.

4.2.2 암호화 관련 주요 내용

❍ 전자정부법 제56조

제56조(정보통신망 등의 보안대책 수립·시행)

① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.

② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.

③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

❍ 전자정부법시행령 제69조, 제70조

제69조(전자문서의 보관·유통 관련 보안조치)

① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.

1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행

② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.

③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치에 관하여 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

제70조(보안조치 이행 여부의 확인)

① 국가정보원장은 법 제56조제3항에 따라 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부를 확인하는 경우 점검항목·절차·시기 등에 관하여 해당 행정기관의 장에게 미리 통보하여야 한다.

② 국가정보원장은 이행 여부의 확인 결과 신속한 시정이 필요하다고 판단하는 경우에는 행정기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 요청을 받은 행정기관의 장은 특별한 사유가 없으면 이에 따라야 한다.

③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치의 이행 여부 확인에 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

4.3 정보통신망 이용촉진 및 정보보호 등에 관한 법률

4.3.1 적용 대상

❍ 정보통신서비스 제공자(기간통신사업자, 별정통신사업자, 부가통신사업자), 방송사업자 등이 적용 대상에 해당한다.

4.3.2 암호화 관련 주요 내용

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조

제28조(개인정보의 보호조치)

① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 제4항 및 6항

제15조(개인정보의 보호조치)

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장
2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

❍ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 제6항에 따른 '개인정보의 기술적·관리적 보호조치 기준 제6조' (방송통신위원회 고시 제2012-50호)

제6조(개인정보의 암호화)

① 정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

4.4 전자금융거래법, 전자금융감독규정

4.4.1 적용 대상

❍ 은행, 금융투자업자, 증권금융회사, 종합금융회사, 명의개서대행회사, 보험회사, 상호저축은행 및 그 중앙회, 신용협동조합 및 그 중앙회, 여신전문금융회사, 농협은행 및 조합, 수산업 협동조합 및 그 중앙회의 신용사업부문, 산림조합 및 그 중앙회의 신용사업부문, 체신관서, 새마을금고 및 새마을금고연합회, 한국거래소, 한국예탁결제원, 금융지주회사 및 전산자회사, 전자금융업자 기타 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자를 적용 대상으로 한다.

4.4.2 암호화 관련 주요 내용

❍ 전자금융거래법 제21조

제21조(안전성의 확보의무)

① 금융기관·전자금융업자 및 전자금융보조업자(이하 "금융기관등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.

② 금융기관등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다. <개정 2008.2.29>

③ 금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 「전자서명법」 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다. <개정 2008.2.29>

❍ 전자금융감독규정 제15조, 제17조, 제31조, 제32조, 제33조, 제34조, 제60조

제15조(해킹 등 방지대책)

① 금융기관 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 단말기에서 제1호의 규정에 따른 정보보호시스템을 우회한 인터넷 등 외부통신망(무선통신망을 포함한다) 접속 금지

② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 정보보호시스템에 사용하는 정보보호제품은 국가기관의 평가·인증을 받은 장비를 사용할 것
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
4. 정보보호시스템의 원격관리를 금지하고 주기적으로 작동 상태를 점검할 것
5. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융기관 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.

⑤ 금융기관 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 사고에 대비하여 정보처리시스템 및 정보통신망에 대해서 매년 취약점을 분석·평가하고 그 이행계획을

수립·시행하여야 한다.

⑥ 금융기관 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 소관 부서장의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 지정된 업무 용도와 사용 지역(zone) 이외 무선통신망 접속을 차단하기 위한 차단 시스템 구축 및 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

제17조(홈페이지 등 공개용 웹서버 관리대책)

① 금융기관 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것

2. 공개용 웹서버에 접근할 수 있는 사용자계정을 업무관련자만 접속할 수 있도록 제한하고 불필요한 계정 또는 서비스번호(port)는 삭제할 것(다만, 사용자계정은 아이디 및 비밀번호 이외에 제37조에 따른 공인인증서 등을 추가 인증수단으로 반드시 적용하여야 한다)
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융기관 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 금융기관 또는 전자금융업자는 홈페이지 등 공개용 웹서버에 대해 6개월마다 취약점을 분석·평가하고 그 이행계획을 수립·시행하여야 한다.

④ 금융기관 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 다음 각 호에 대하여 적절하게 대응 조치하여야 한다.

1. 악의적인 명령어 주입 공격(SQL injection)
2. 업로드 취약점

3. 취약한 세션 관리(cookie injection)
4. 악의적인 명령 실행(XSS)
5. 버퍼 오버플로우(buffer overflow)
6. 부적절한 파라미터(parameter)
7. 접근통제 취약점
8. 서버설정과 관련한 부적절한 환경설정 취약점

⑤ 금융기관 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

제31조(암호프로그램 및 키 관리 통제)

① 금융기관 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다.

② 금융기관 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

제32조(내부사용자 비밀번호 관리)

금융기관 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 제12조제3호에 따라 비밀번호 부여 및 변경
   나. 비밀번호 보관 시 암호화
   다. 시스템마다 관리자 비밀번호를 다르게 부여
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리)

① 금융기관 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.

② 금융기관 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시

해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)

4. 금융기관이 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

제34조(전자금융거래 시 준수사항)

① 금융기관 또는 전자금융업자는 다음의 경우를 제외하고는 전자자금이체 시 보안카드를 포함한 일회용 비밀번호를 적용하여야 한다.

1. 자동화기기(CD/ATM)를 이용한 자금이체의 경우
2. 제휴 금융기관에서 실명 확인 후 개설된 증권계좌와 연계된 본인명의의 실명확인 계좌로 이체하는 경우
3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자를 방문하여 등록한 실명 확인된 본인 명의 계좌로 이체하는 경우
4. 신용카드 대출서비스를 실명 확인된 본인명의 계좌로 이체하는 경우
5. 보험회사의 보험금, 대출금 등을 실명 확인된 본인명의의 보험료납입 계좌로 이체하는 경우
6. 법인이 금융기관과 연결된 전용회선을 이용하여 전자자금이체를 하는 경우
7. 등록금, 원서접수비 등 본인확인이 가능하고 입금계좌가 지정되어 있는 경우
8. 그 밖에 금융감독원장이 필요하다고 인정하는 경우

② 금융기관 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 보안성심의를 받은 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 해킹 등 침해행위로부터 전자금융거래를 보호하기 위해 이용자의 전자적 장치에 보안프로그램 설치 등 보안대책을 적용할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램을 해제할 수 있다)
4. 전자금융거래에 사용되는 일회용 비밀번호(OTP를 포함한다. 이하 이 조에서 같다) 등의 접근매체를 발급받기 위해서는 반드시 본인 실명증표를 확인한 후 교부할 것
5. 전자금융거래수단이 되는 매체와 일회용 비밀번호 등 거래인증수단이 되는 매체를 분리하여 사용할 것

6. 비밀번호 개수가 한정된 일회용 비밀번호 사용 시에 비밀번호 입력 오류가 발생하거나 일회용 비밀번호를 입력하지 않고 비정상적으로 거래를 종료하면, 다음 거래 시 동일한 비밀번호를 요구할 것
7. 금융기관 또는 전자금융업자는 전자금융거래에서 이용자에 게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

제60조(외부주문등에 대한 기준)

① 금융기관 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 정보처리시스템 설치장소에 대한 통제
2. 금융기관과 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지

Ⅲ 개인정보 암호화 방식

제1절 전송시 암호화

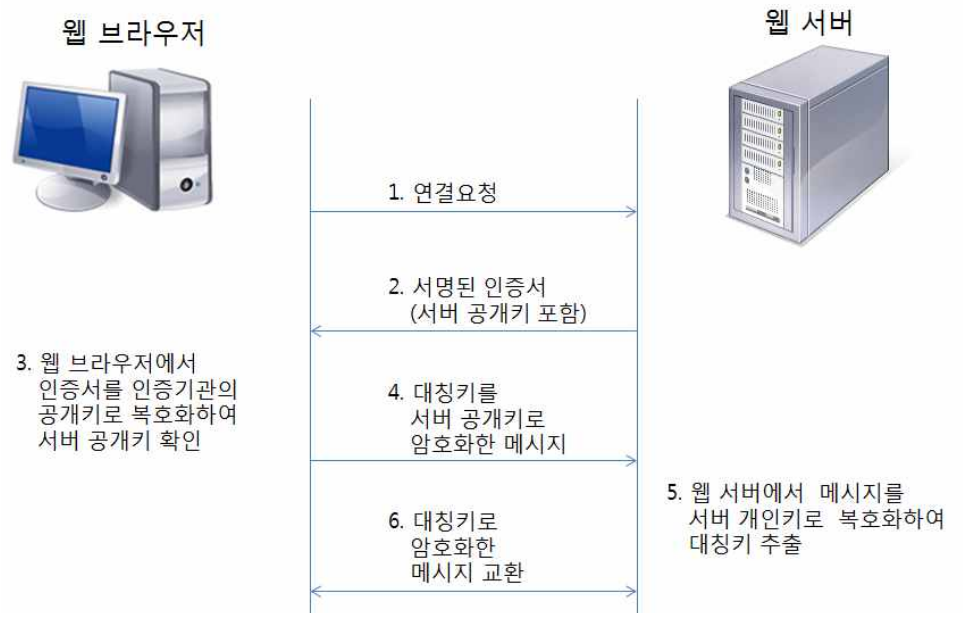
1.1 웹서버와 클라이언트 간 암호화

- 웹서버와 클라이언트 간 개인정보 전송시 암호화를 위하여 공인인증기관이 발급한 서버 인증서를 설치한 보안서버를 사용하는 방식으로 웹브라우저에 기본적으로 내장된 SSL/TLS 프로토콜로 접속하는 SSL 방식과 웹브라우저에 보안 프로그램을 설치하여 접속하는 응용프로그램 방식으로 구분할 수 있다.
- SSL 방식은 웹페이지 전체를 암호화(웹페이지내 이미지 포함)하며 응용프로그램 방식은 특정 데이터만을 선택적으로 암호화할 수 있지만, 보안서버와 웹브라우저에 부가적인 프로그램을 설치해야 한다.
- 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용해야 한다.

1.1.1 SSL 방식

- SSL 방식은 전송 계층(Transport Layer)을 기반으로 한 응용 계층(Application Layer)에서 암호화를 수행한다. 암호키교환은 비대칭키 암호 알고리즘을 이용하고, 기밀성을 위한 암호화는 대칭키 암호 알고리즘을 이용하며 메시지의 무결성은 메시지 인증 코드(해쉬함수)를 이용하여 보장한다.
- 인터넷 쇼핑이나 인터넷 뱅킹 시 계좌정보 및 주민등록번호 등과 같은 중요한 정보를 입력할 때, 거래당사자의 신원 및 거래내용의 위·변조 여부를 확인하고 중요 정보가 제3자에게 유출되는 것을 막기 위해 SSL/TLS와 같은 통신 암호기술을 이용할 수 있다.
- <그림 3>은 인증기관으로부터 인증서를 발급받은 웹서버와 사용자의 웹브라우저 간 SSL/TLS를 이용한 보안 통신의 개념을 간단하게 소개하고 있다. 사용자가 웹서버에 처음 접속하면 인증서 및 통신 암호화에 이용할 암호키를 생성하기 위한 정보를 공유하고, 이후 공유된 정보를 통해 생성된 암호키를 이용하여 데이터를 암호화하여 전송한다.

❍ SSL/TLS 통신을 하는 경우에는 로그인 페이지 등 보안이 필요한 웹페이지에 접속하면 웹브라우저 하단 상태 표시줄에 자물쇠 모양의 표시를 확인할 수 있다.



<그림 3> 웹서버와 웹브라우저 간의 SSL/TLS 통신 구조

1.1.2 응용프로그램 방식

❍ 응용프로그램 방식은 별도의 모듈을 서버와 클라이언트에 설치해야 하며 필요한 데이터만 암호화하여 전달할 수 있다. 이를 위해 웹서버 프로그램에 대한 수정작업이 필요하며, 응용프로그램 방식을 제공하는 솔루션에 따라 수정작업의 범위가 달라질 수 있다.

❍ 보안서버를 구현한 웹서버에 사용자가 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인정보를 암호화하여 통신이 이루어진다. 웹브라우저의 확장기능인 플러그인 형태로 구현되며 웹사이트 접속 시 초기화면이나 로그인 후 윈도우 화면 오른쪽 하단 작업표시줄 알림영역을 확인하여 프로그램이 실행되고 있음을 알 수 있다.

1.2 개인정보처리시스템 간 암호화

❍ 개인정보처리시스템 간에 개인정보를 전송할 때 암호화를 지원하기 위하여 공중망을 이용한 VPN(가상사설망)을 구축할 수 있다.

❍ VPN은 기반이 되는 보안 프로토콜의 종류에 따라 IPsec VPN 방식, SSL VPN 방식, SSH VPN 방식 등으로 구분할 수 있으며, 개인정보처리시스템 간의 통신에서 사용할 수 있는 VPN 전송 방식의 특징을 간단히 비교하면 [표 2]와 같다.

[표 2] 개인정보처리시스템 간 전송시 암호화 방식 비교

방식	VPN 서버부하	NAT 통과
IPsec VPN	낮음	어려움
SSL VPN	다소 높음	쉬움
SSH VPN	다소 높음	쉬움

※ NAT(Network Address Translation) : 사설 IP 주소를 공인 IP 주소로 바꿔주는데 사용하는 통신망의 주소변환기

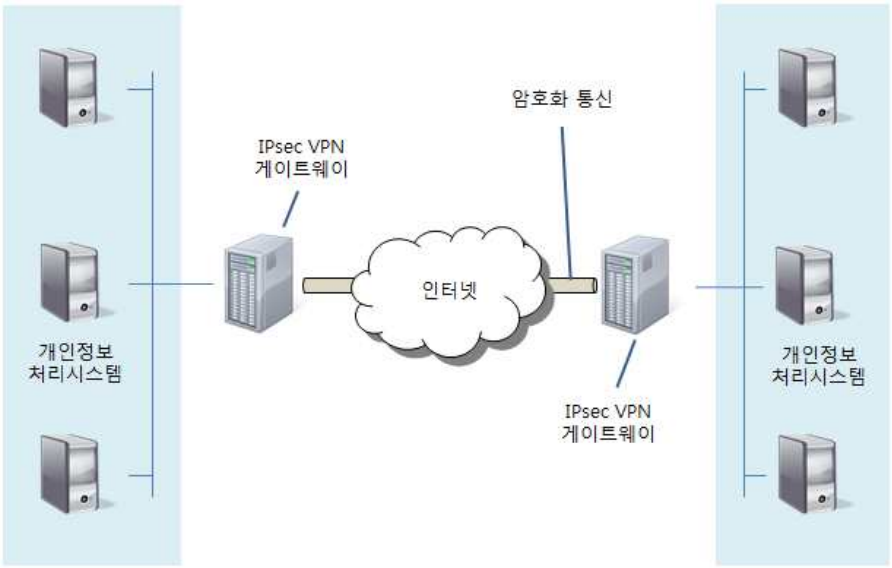
❍ VPN은 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고 수신측에서 이를 복호화 하는 방식으로 송·수신 정보에 대한 기밀성 및 무결성을 보장하며, 그 외에도 데이터 출처 인증, 재전송 방지, 접근제어 등 다양한 보안 기능을 제공한다.

1.2.1 IPsec VPN 방식

❍ IPsec VPN 방식은 응용프로그램을 수정할 필요가 없으나 IPsec 패킷의 IP 주소를 변경해야 하는 NAT와 같이 사용하기 어려운 점이 있다. 사용자 인증이 필요 없으므로 VPN 장비 간 서로 인증이 된 경우, 사용자는 다른 인증절차를 거치지 않아도 된다.

❍ IPsec VPN 방식의 구조는 게이트웨이 대 게이트웨이, 호스트 대 게이트웨이, 호스트 대 호스트로 구분할 수 있다. 게이트웨이 대 게이트웨이는 네트워크 간의 암호화 통신, 호스트 대 게이트웨이는 개인정보처리시스템과 네트워크 간의 암호화 통신, 호스트 대 호스트는 개인정보처리시스템 간의 암호화 통신을 설정할 수 있다.

❍ <그림 4>는 게이트웨이 대 게이트웨이 IPsec VPN 방식을 이용하여 인터넷을 통과하는 암호화 통신을 보여준다.

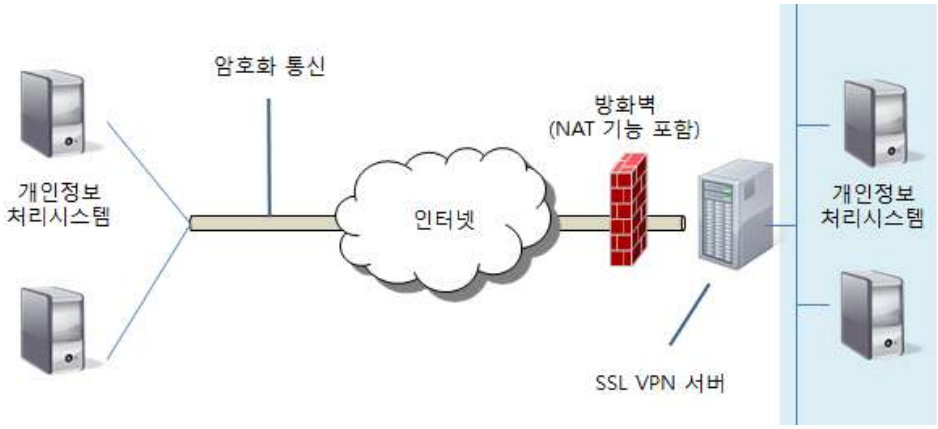


<그림 4> IPsec VPN 방식(게이트웨이 대 게이트웨이)의 개념도

1.2.2 SSL VPN 방식

❍ SSL VPN 방식은 응용프로그램 수준에서 SSL/TLS을 구현하는 것이 일반적이며 NAT를 사용할 수 있다. SSL/TLS는 메모리 소비가 많으므로 동시 접속이 많은 대용량 처리에서 성능 저하가 발생할 수 있다. 하지만 개별 사용자 인증이 필요한 경우 SSL VPN 방식이 좋은 선택이 될 수 있다.

❍ <그림 5>는 SSL VPN 방식에서 SSL VPN 서버를 거친 개인정보처리시스템 간의 암호화 통신을 보여준다. 이러한 구조는 방화벽 외부에 위치한 개인정보처리시스템과 SSL VPN 서버가 설치된 LAN에 위치한 개인정보처리시스템 간의 통신에 이용이 가능하다.

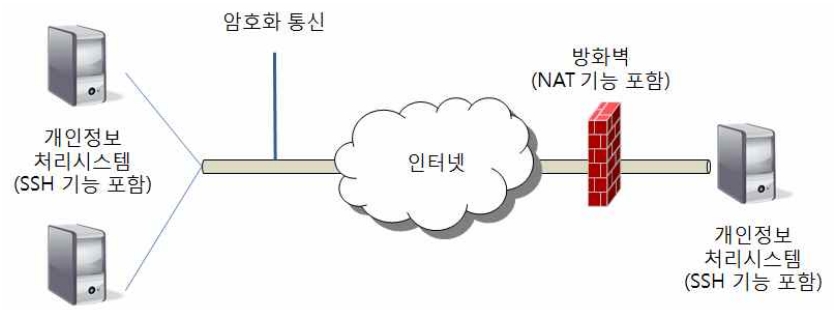


<그림 5> SSL VPN 방식의 개념도

1.2.3 SSH VPN 방식

❍ SSH VPN 방식은 응용계층의 VPN 기술로서 원격 단말기에서 접속하는 경우에 주로 이용되며 SSH를 이용한 파일 전송 및 파일 복사 프로토콜(예: SFTP, SCP)을 이용할 수 있다. 오픈소스 SSH의 일종인 OpenSSH의 경우 프락시 방식의 VPN 서버로 구성할 수도 있다.

❍ <그림 6>은 SSH VPN 방식에서 개인정보처리시스템 간의 암호화 통신을 보여준다. 각 개인정보처리시스템에 설치된 SSH 기능을 사용하여 VPN을 구성할 수 있다.



<그림 6> SSH VPN 방식의 개념도

TIP
- 개인정보처리시스템 간 전송시 공중망과 분리된 전용선을 사용하면 암호화에 상응하는 보안성을 제공할 수 있다.

1.3 개인정보취급자 간 암호화

❍ 개인정보취급자 간에 개인정보를 전송할 때 주로 이메일을 이용하게 된다. 이메일은 네트워크를 통해 전송되는 과정에서 공격자에 의해 유출되거나 위조될 가능성이 있다. 이러한 위협으로부터 이메일로 전송되는 메시지를 보호하기 위해서 PGP 또는 S/MIME을 이용하는 이메일 암호화 방식과 암호화된 파일을 이메일에 첨부하여 전송하는 이메일 첨부문서 암호화 방식이 있다.

• 개인정보취급자 간에 이메일을 사용하지 않고 직접 파일을 전송하고자 하는 경우는 개인정보처리시스템 간 전송시 암호화 방식의 VPN 기능을 적용할 수 있다.

❍ 개인정보취급자 간에 이메일을 전송할 때 사용되는 암호화 방식의 특징은 [표 3]과 같다.

[표 3] 개인정보취급자 간 전송시 암호화 방식 비교

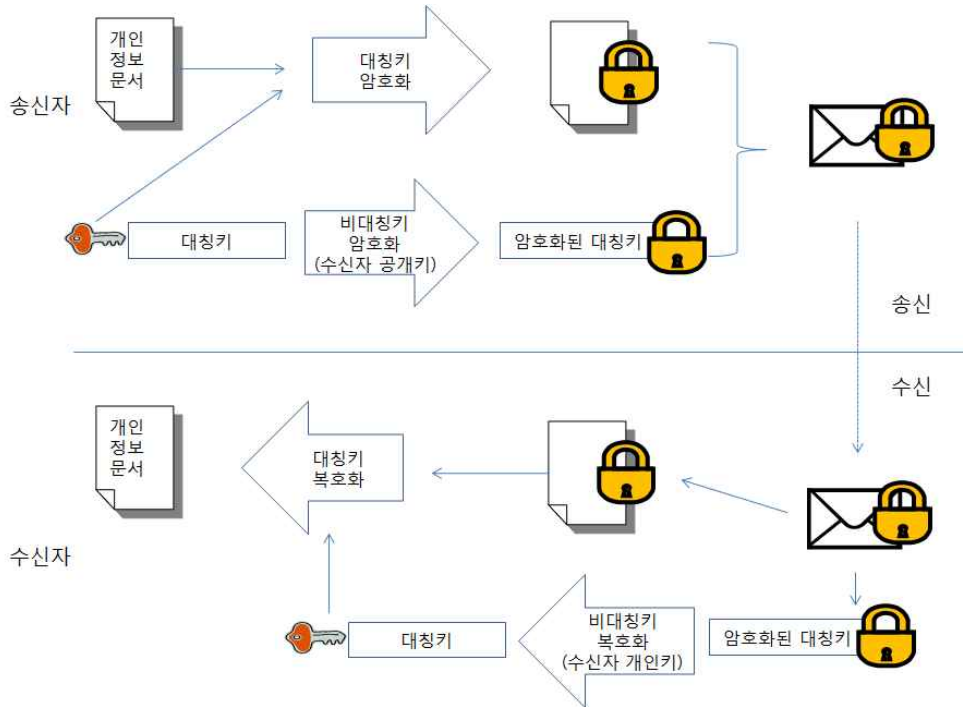
방식		공인인증서 필요 여부	표준형식
이메일 암호화	PGP	필요하지 않음	PGP 자체정의
	S/MIME	필요함	X.509, PKCS#7
이메일 첨부문서 암호화		필요하지 않음	없음

❍ S/MIME은 공개키를 포함한 공인인증서를 발급받고 등록해야 하는 번거로움이 있다. 이에 비해 PGP의 경우 개인 간의 신뢰를 바탕으로 공개키를 등록하거나 안전한 채널로 미리 확보하는 방법을 사용할 수 있다.

1.3.1 이메일 암호화 방식

❍ 이메일 암호화 방식은 송·수신되는 이메일의 내용을 암호화함으로써 메일 내 중요 개인정보의 유출을 방지하는 것이며, 대표적인 이메일 보안 프로토콜로는 PGP와 S/MIME이 있다. <그림 7>은 이메일 암호화 방식의 처리 과정을

보여준다.



<그림 7> 이메일 암호화 방식의 개념도

❍ PGP는 다양한 응용프로그램에 적용하여 문서, 이메일, 파일, 파일시스템, 디스크 등을 암호화할 수 있다.

❍ S/MIME은 인증, 메시지 무결성, 부인방지, 메시지 암호화 등에 사용되며 대부분의 이메일 클라이언트에서 기본적으로 지원한다. S/MIME을 사용하기 위해서는 공인인증기관이 발행한 공인인증서가 있어야 한다.

1.3.2 이메일 첨부문서 암호화 방식

❍ 업무용 컴퓨터에서 주로 사용하는 문서 도구(예: 흔글, MS 워드 등)의 자체 암호화 방식, 암호 유틸리티를 이용한 암호화 방식 등을 통해 암호화한 파일을 이메일의 첨부문서로 송·수신할 수 있다.[1)]

❍ 이메일을 송·수신할 개인정보취급자 간에는 암호키(또는 비밀번호)를 안전하게 공유하여야 한다.

1) 파일 암호화 방식은 'III장 2.2 업무용 컴퓨터 암호화'를 참고

제2절 저장시 암호화

2.1 개인정보처리시스템 암호화

2.1.1 개요

❍ 개인정보를 처리하고 관리하는 개인정보처리시스템은 DB에 저장된 개인정보를 암호화하여 저장함으로써 개인정보의 변경, 파괴 및 유출을 방지해야 한다.

❍ 개인정보처리시스템의 DB를 암호화할 수 있는 방식은 암·복호화 모듈의 위치와 암·복호화 모듈의 요청 위치의 조합에 따라 [표 4]와 같이 구분할 수 있다.

[표 4] 개인정보처리시스템 암호화 방식의 구분

방식	암·복호화 모듈 위치	암·복호화 요청 위치	주요 내용
응용 프로그램 자체 암호화	어플리케이션 서버	응용 프로그램	• 암·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고, 응용프로그램에서 해당 암·복호화 모듈을 호출하는 방식 • DB 서버에 영향을 주지 않아 DB 서버의 성능 저하가 적은 편이지만 구축시 응용프로그램 전체 또는 일부 수정 필요 • 기존 API 방식과 유사
DB 서버 암호화	DB 서버	DB 서버	• 암·복호화 모듈이 DB 서버에 설치되고 DB 서버에서 암·복호화 모듈을 호출하는 방식 • 구축 시 응용프로그램의 수정을 최소화할 수 있으나 DB 서버에 부하가 발생하며 DB 스키마의 추가 필요 • 기존 Plug-In 방식과 유사
DBMS 자체 암호화	DB 서버	DBMS 엔진	• DB 서버의 DBMS 커널이 자체적으로 암·복호화 기능을 수행하는 방식 • 구축 시 응용프로그램 수정이 거의 없으나, DBMS에서 DB 스키마의 지정 필요 • 기존 커널 방식(TDE)과 유사

방식	암·복호화 모듈 위치	암·복호화 요청 위치	주요 내용
DBMS 암호화 기능 호출	DB 서버	응용 프로그램	• 응용프로그램에서 DB 서버의 DBMS 커널이 제공하는 암·복호화 API를 호출하는 방식 • 구축 시 암·복호화 API를 사용하는 응용프로그램의 수정이 필요 • 기존 커널 방식(DBMS 함수 호출)과 유사
운영체제 암호화	파일 서버	운영체제 (OS)	• OS에서 발생하는 물리적인 입출력(I/O)을 이용한 암·복호화 방식으로 DBMS의 데이터파일 암호화 • DB 서버의 성능 저하가 상대적으로 적으나 OS, DBMS, 저장장치와의 호환성 검토 필요 • 기존 DB 파일암호화 방식과 유사

• 각 방식의 단점을 보완하기 위하여 두 가지 이상의 방식을 혼합하여 구현하기도 한다. 이 경우, 구축 시 많은 비용이 소요되지만 어플리케이션 서버 및 DB 서버의 성능과 보안성을 높일 수 있다.

❍ 개인정보처리시스템 암호화 방식마다 성능에 미치는 영향이 다르므로 구축 환경에 따라 암호화 방식의 특성, 장단점 및 제약사항 등을 고려하여 DB 암호화 방식을 선택해야 한다. [표 5]는 개인정보처리시스템 암호화 방식의 선택 시 고려해야 할 사항이다.

[표 5] 개인정보처리시스템 암호화 방식 선택 시 고려사항

분 류	항 목
일반적 고려사항	구현 용이성, 구축 비용, 기술지원 및 유지보수 여부
	암호화 성능 및 안전성
	공공기관의 경우, 국가정보원 인증 또는 검증 여부
기술적 고려사항	암·복호화 위치(어플리케이션 서버, DB 서버, 파일서버 등)
	색인검색 가능 유무, 배치처리 가능 여부

- 성능이 매우 중요한 요소가 되는 환경에서 DB 서버 암호화 방식을 고려하는 경우에는 반드시 벤치마킹 테스트(BMT) 등을 수행하여, 최적의 솔루션을 선택하는 것이 바람직하다.

❍ 공공기관에서는 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용해야 한다.[2)]

❍ 암·복호화 모듈의 위치와 암·복호화 요청 위치에 따라 어플리케이션 서버 또는 DB 서버의 성능에 영향을 미칠 수 있다. 예를 들어, DB 서버 암호화 방식은 암·복호화 시 DB 서버의 자원을 추가적으로 사용하므로 대량의 트랜잭션 작업에서 DB 서버의 성능 저하가 발생할 수 있다.

❍ 현재 운영 중이거나 향후 개발 예정인 개인정보처리시스템의 목적 및 환경에 맞게 쉽게 구현이 가능한 암호화 방식을 선택해야 한다. 응용프로그램 및 DB 스키마 수정 등을 최소화하고 개발 환경에 맞게 성능을 최대화할 수 있도록 해야 한다.

❍ DB 암호화의 안전성을 확보하기 위해서는 안전한 암호키의 관리가 필요하다. 암호화된 개인정보가 유출되더라도 복호화 할 수 없도록 암호키에 대한 추가적인 보안과 제한된 관리자만 허용하도록 하는 기술의 적용을 권고한다.

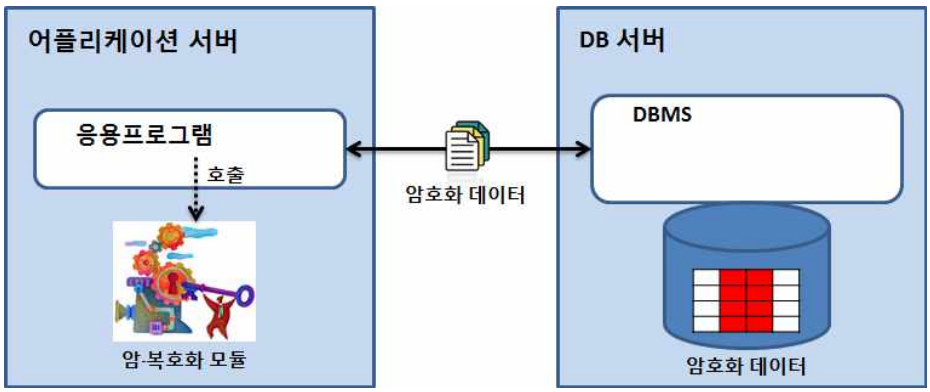
2) IT보안인증사무국(http://service1.nis.go.kr)의 검증필 암호 모듈 또는 제품 확인이 가능함

2.1.2 응용프로그램 자체 암호화 방식

❍ 응용프로그램 자체 암호화 방식은 <그림 8>과 같이 암·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고 응용프로그램에서 암·복호화 모듈을 호출하는 방식이다.

❍ DB 서버에는 영향을 주지 않지만 어플리케이션 서버에 암·복호화를 위한 추가적인 부하가 발생하며, 구축 시 응용프로그램 전체 또는 일부 수정이 필요하다.

❍ 추가적으로 어플리케이션 서버와 DB 서버 간의 통신에서 암호화된 개인정보의 전송을 보장할 수 있다.



<그림 8> 응용프로그램 자체 암호화 방식의 개념도

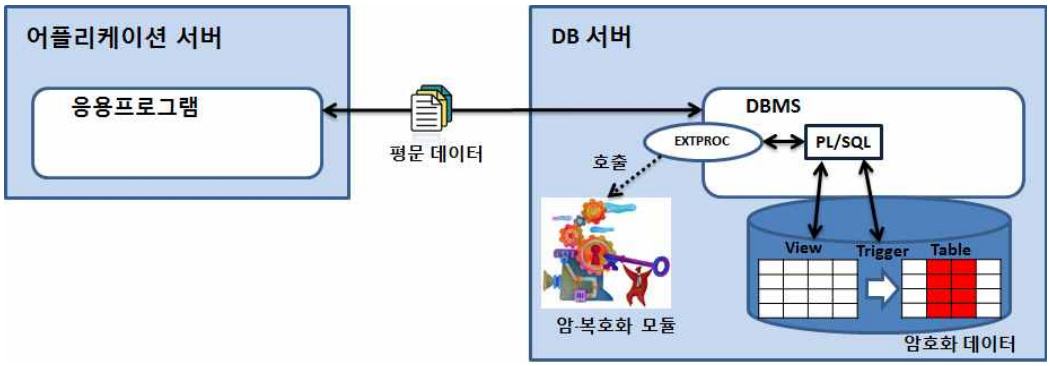
❍ 응용프로그램 자체 암호화 방식의 주요 특성은 [표 6]과 같다.

[표 6] 응용프로그램 자체 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	어플리케이션 서버
암·복호화 요청	응용프로그램
DB 서버의 부하	없음(어플리케이션 서버에 부하 발생)
색인 검색	일치검색 가능 별도 색인 테이블 생성을 통해 가능(추가 작업 필요)
배치 처리	가능
응용프로그램 수정	필요함
DB 스키마 수정	거의 필요하지 않음(암호화에 따른 속성 타입이나 길이의 변경이 필요할 수 있음)

2.1.3 DB 서버 암호화 방식

- DB 서버 암호화 방식은 <그림 9>와 같이 암·복호화 모듈이 DB 서버에 설치되고 DBMS에서 플러그인(plug-in)으로 연결된 암·복호화 모듈을 호출하는 방식이다.
- 응용프로그램의 수정이 거의 필요하지 않아 구현 용이성이 뛰어나지만, 기존 DB 스키마와 대응하는 뷰(view)를 생성하고 암호화할 테이블을 추가하는 작업이 필요하다.
- 어플리케이션 서버의 성능에는 영향을 주지 않지만 DBMS에서 DB 서버의 암·복호화 모듈을 플러그인으로 호출할 때 추가적인 부하가 발생하여 성능이 저하될 수 있다.



<그림 9> DB 서버 암호화 방식의 개념도

- DB 서버 암호화 방식의 주요 특성은 [표 7]과 같다.

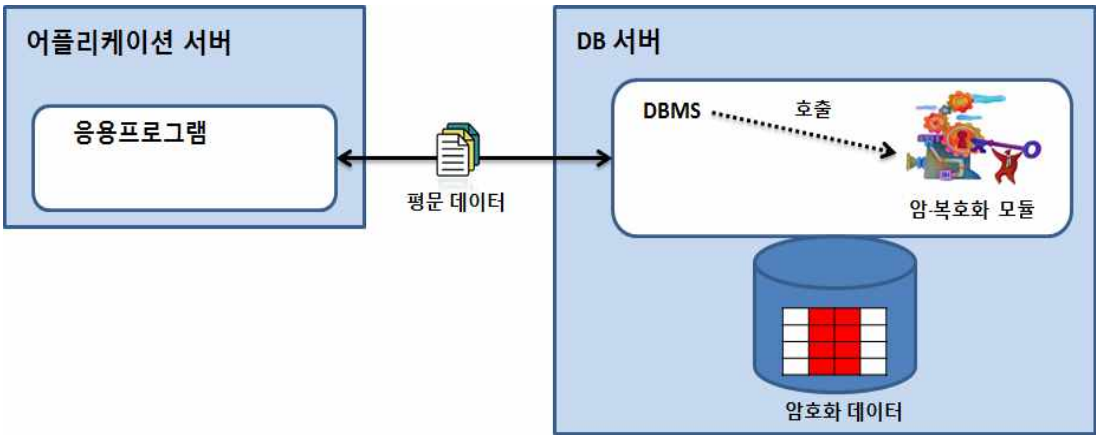
[표 7] DB 서버 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	DB 서버
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능(대량의 배치 트랜잭션 처리는 많이 느릴 수 있음)
응용프로그램 수정	기본적으로 수정 없이 적용할 수 있으나, 제약사항 또는 성능 문제가 있는 경우 수정이 필요함
DB 스키마 수정	필요함

2.1.4 DBMS 자체 암호화 방식

❍ DBMS 자체 암호화 방식은 <그림 10>과 같이 DBMS에 내장되어 있는 암호화 기능(TDE : Transparent Data Encryption)을 이용하여 암·복호화 처리를 수행하는 방식이다.

❍ DBMS 커널 수준에서 처리되므로 기존 응용프로그램의 수정이나 DB 스키마의 변경이 거의 필요하지 않고 DBMS 엔진에 최적화된 성능을 제공할 수 있다.



<그림 10> DBMS 자체 암호화 방식의 개념도

❍ DBMS 자체 암호화 방식의 주요 특성은 [표 8]과 같다.

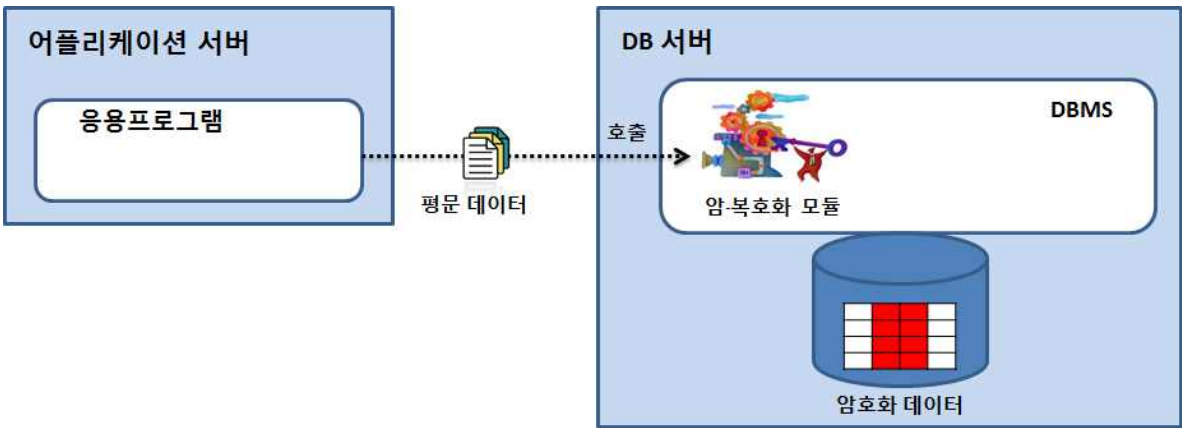
[표 8] DBMS 자체 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	DBMS 엔진
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능
응용프로그램 수정	필요하지 않음
DB 스키마 수정	거의 필요하지 않음(암호화할 DB 스키마 지정 필요)

2.1.5 DBMS 암호화 기능 호출 방식

❍ DBMS 암호화 기능 호출 방식은 <그림 11>과 같이 DBMS가 자체적으로 암·복호화 기능을 수행하는 API를 제공하고 해당 함수를 사용하기 위해 응용프로그램에서 호출하는 방식이다.

❍ 암·복호화 API를 사용하는 응용프로그램의 수정이 필요하고, DB 서버에 추가적인 부하가 발생할 수 있다.



<그림 11> DBMS 암호화 기능 호출 방식의 개념도

❍ DBMS 암호화 기능 호출 방식의 주요 특성은 [표 9]와 같다.

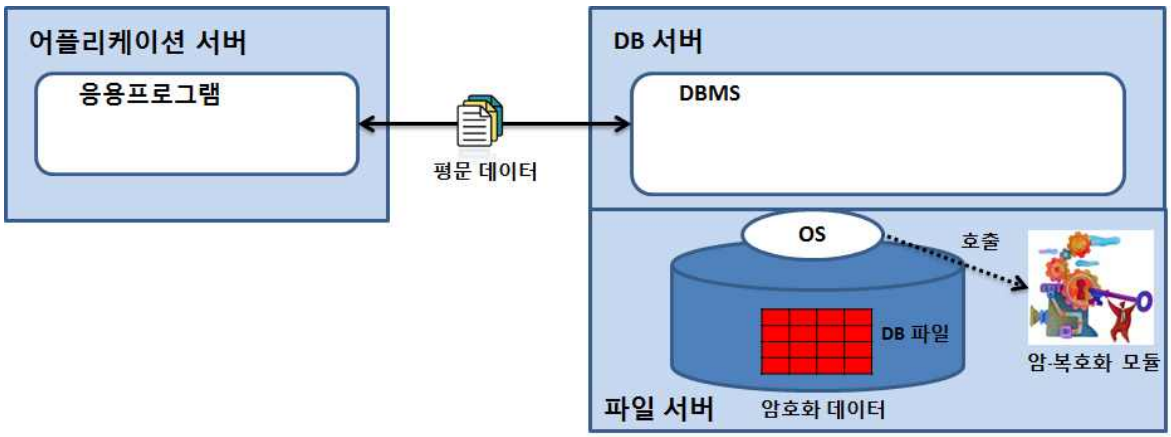
[표 9] DBMS 암호화 기능 호출 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	DB 서버
암·복호화 요청	응용프로그램
DB 서버의 부하	있음
색인 검색	불가능
배치 처리	가능(대량의 배치 트랜잭션 처리는 많이 느릴 수 있음)
응용프로그램 수정	수정 필요
DB 스키마 수정	일부 수정 필요

2.1.6 운영체제 암호화 방식

❍ 운영체제 암호화 방식은 <그림 12>와 같이 OS에서 발생하는 입출력 시스템 호출을 이용한 암·복호화 방식으로서 DB 파일 자체를 암호화한다.

❍ 응용프로그램이나 DB 스키마의 수정이 필요하지 않지만 DB 파일 전체를 암호화하는데 따른 파일 서버 및 DB 서버에 추가적인 부하가 발생할 수 있다.



<그림 12> 운영체제 암호화 방식의 개념도

❍ 운영체제 암호화 방식의 주요 특성은 [표 10]과 같다.

[표 10] 운영체제 암호화 방식의 주요 특성

항 목	주요 내용
암·복호화 모듈	파일 서버(또는 DB 서버)
암·복호화 요청	운영체제
DB 서버의 부하	있음
색인 검색	가능
배치 처리	가능
응용프로그램 수정	필요하지 않음
DB 스키마 수정	필요하지 않음

2.2 업무용 컴퓨터 암호화

2.2.1 개요

❍ 업무용 컴퓨터에서는 보조저장매체에 저장된 개인정보의 보호를 위하여 개별 문서 파일 단위로 암호화(파일 암호화) 또는 디렉터리 단위로 암호화(디스크 암호화)를 수행해야 한다.

❍ 파일 암호화는 업무용 컴퓨터에 저장된 개인정보에 대한 보호뿐만 아니라 개인정보취급자 간에 네트워크상으로 파일을 안전하게 전송하기 위한 방식으로도 사용할 수 있다.

❍ 업무용 컴퓨터에서 가능한 암호화 방식은 [표 11]과 같이 구분할 수 있다.

[표 11] 업무용 컴퓨터 암호화 방식의 구분

방식	주요 내용
문서 도구 자체 암호화	• 업무용 컴퓨터에서 사용하는 문서도구의 자체 암호화 기능을 통하여 개인정보 파일 암호화
암호 유틸리티를 이용한 암호화	• 업무용 컴퓨터의 OS에서 제공하는 파일 암호 유틸리티 또는 파일 암호 전용 유틸리티를 이용한 개인정보 파일의 암호화
DRM (Digital Right Management)	• DRM을 이용하여 다양한 종류의 파일 및 개인정보 파일의 암호화
디스크 암호화	• 디스크에 데이터를 기록할 때 자동으로 암호화하고, 읽을 때 자동으로 복호화하는 기능을 제공함 • 디스크 전체 또는 일부 디렉터리를 인가되지 않은 사용자에게 보이지 않게 설정하여 암호화 여부와 관계없이 특정 디렉터리 보호 가능

❍ 업무용 컴퓨터 암호화 방식의 특징을 간단히 비교하면 [표 12]와 같다.

[표 12] 업무용 컴퓨터 암호화 방식의 비교

방식	지원 파일 종류	
	특정 문서*	일반 파일**
문서 도구 자체 암호화	지원함	지원하지 않음
암호 유틸리티를 이용한 암호화	지원함	지원함
DRM	지원함	지원함
디스크 암호화	지원함	지원함

*특정문서: 흔히 사용하는 문서 도구(예: ㅎ글, MS 워드 등)로 작성한 파일
**일반문서: 특정 문서 이외의 문서(예: 텍스트 파일, 이미지 파일 등)

2.2.2 문서 도구 자체 암호화 방식

❍ 업무용 컴퓨터에서 주로 사용하는 문서 도구(예를 들어, 흔글, MS 워드 등)에서는 자체 암호화 기능을 통하여 개인정보 파일을 암호화할 수 있다.

2.2.3 암호 유틸리티를 이용한 암호화 방식

❍ 업무용 컴퓨터에서는 해당 컴퓨터의 OS에서 제공하는 파일암호 유틸리티 또는 파일암호 전용 유틸리티를 이용하여 개인정보 파일 또는 디렉터리를 암호화할 수 있다.

2.2.4 DRM 방식

❍ DRM은 조직 내부에서 생성되는 전자문서를 암호화하고 해당 문서를 접근 및 사용할 수 있는 권한을 지정함으로써 허가된 사용자만 중요 문서(개인정보 문서, 기밀문서 등)를 사용하게 하는 기술이다.

❍ DRM은 중요 문서 외에 다양한 종류의 멀티미디어 콘텐츠(음악, 사진, 동영상, 이미지 등)에 대한 보안 기능을 제공할 수 있다.

❍ DRM으로 암호화된 문서는 DRM 클라이언트가 없는 PC에서는 열람이 불가능하며, 열람 중에도 파일이 복호화 되지 않고 암호화 상태를 유지한다.

2.2.5 디스크 암호화 방식

❍ 디스크 암호화는 디스크에 데이터를 기록할 때 자동으로 암호화하고, 주기억장치로 읽을 때 자동으로 복호화하는 방식이다.

❍ 휴대용 보조기억매체는 개방된 장소에 놓일 수 있기 때문에 적절한 물리적 보안을 제공하기 어려움이 있다. 따라서 휴대용 보조기억매체는 저장된 개인정보의 기밀성을 위해 디스크 암호화 솔루션을 이용하여 암호화하기를 권고한다.

Ⅳ 개인정보 암호화 적용 사례

제1절 전송시 암호화

1.1 웹서버와 클라이언트 간 암호화 사례

1.1.1 아파치(Apache) 웹서버를 이용한 SSL 방식의 설정

- 대표적인 오픈소스 웹서버 소프트웨어인 아파치에서 설정파일인 'httpd.conf'를 변경하여 SSL/TLS를 설정할 수 있다. 이 설정파일에는 공인인증서의 위치, 서버용 인증서 위치, 공개키와 개인키의 위치 등이 들어가며 SSL/TLS에서 사용하는 암호 알고리즘을 정해준다.
- 웹브라우저가 SSL 방식으로 웹서버에 연결된 경우, <그림 13>과 같이 웹브라우저 주소창 또는 하단의 상태표시줄에 자물쇠 표시가 나타나게 된다.

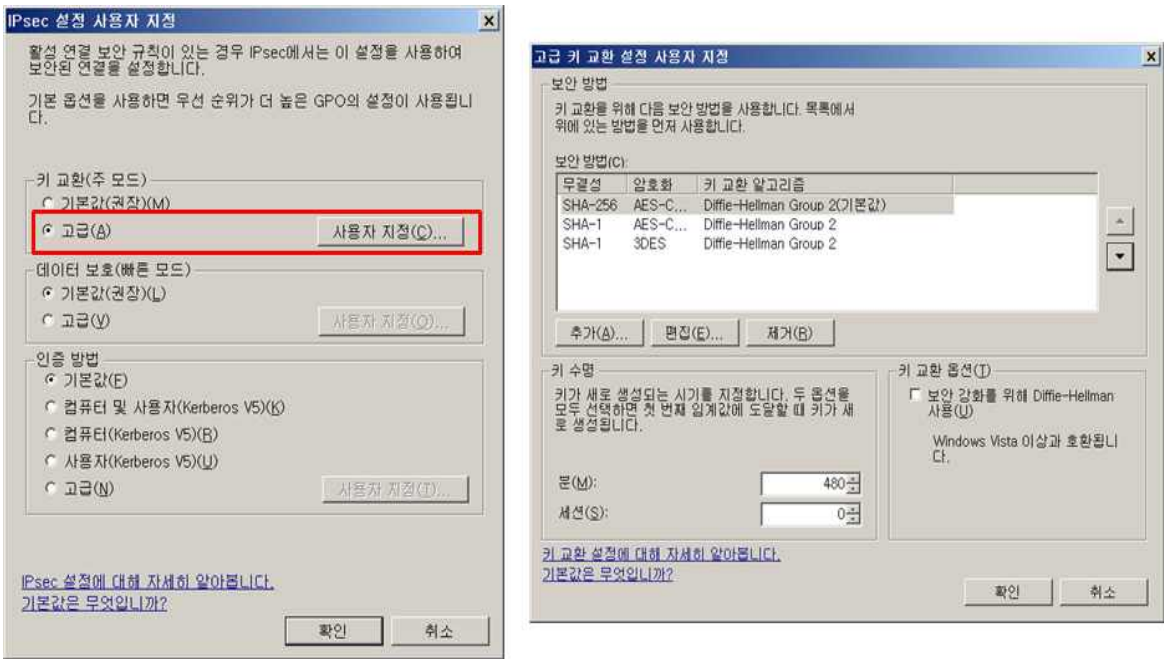
<그림 13> SSL 방식에서 나타나는 웹브라우저 자물쇠 표시

1.2 개인정보처리시스템 간 암호화 사례

1.2.1 윈도우(Windows)에서 IPsec VPN 방식의 설정

- 윈도우를 호스트로 사용하여 IPsec VPN에 접속할 경우, 안전한 암호 알고리즘의 선택을 위해 추가 설정이 필요할 수 있다.
- Windows 7의 제어판 메뉴에서 [윈도우 방화벽] → [고급설정] → [로컬 컴퓨터 고급 보안이 포함된 윈도우 방화벽] → [속성] → [IPsec 설정] → [사용자 지정]을 선택한다.

❍ <그림 14>의 [IPsec 설정 사용자 지정]과 같은 대화창이 나타나면, [키 교환] → [사용자 지정]을 선택하여 [고급 키 교환 설정 사용자 지정]에서 IPsec VPN 방식에 사용할 암호 알고리즘을 변경할 수 있다.



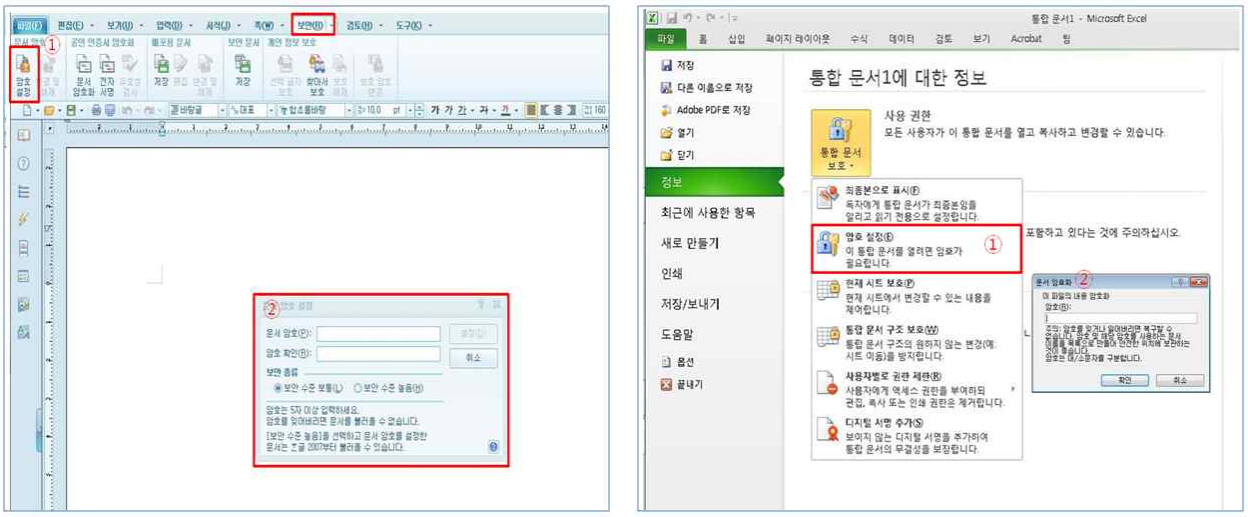
<그림 14> Windows 7에서 IPsec VPN 방식을 위한 암호 알고리즘 설정

1.3 개인정보취급자 간 암호화 사례

1.3.1 첨부문서 암호화 후, 이메일로 전송

❍ 먼저, 응용프로그램의 암호화 기능을 사용하여 암호를 설정한 후, 문서를 저장한다.

- 혼글 2010의 경우, 상단 메뉴의 [보안] → [문서 암호 설정]을 이용하여 문서의 암호를 설정 한 후, [파일] → [저장하기] 메뉴를 이용하여 문서 내용을 저장한다.
- MS 엑셀 2010의 경우 상단 메뉴의 [파일] → [정보] → [통합 문서 보호] → [암호 설정]을 이용하여 문서의 암호를 설정 한 후, [파일] → [저장하기] 메뉴를 이용하여 문서의 내용을 저장한다.



<그림 15> 흔글 2010과 MS 엑셀 2010에서 문서 암호화 설정

❍ 암호화된 문서를 이메일에 첨부한 후, 수신자에게 이메일을 전송한다.

제2절 저장시 암호화

2.1 개인정보처리시스템 암호화 사례

2.1.1 응용프로그램 자체 암호화 방식

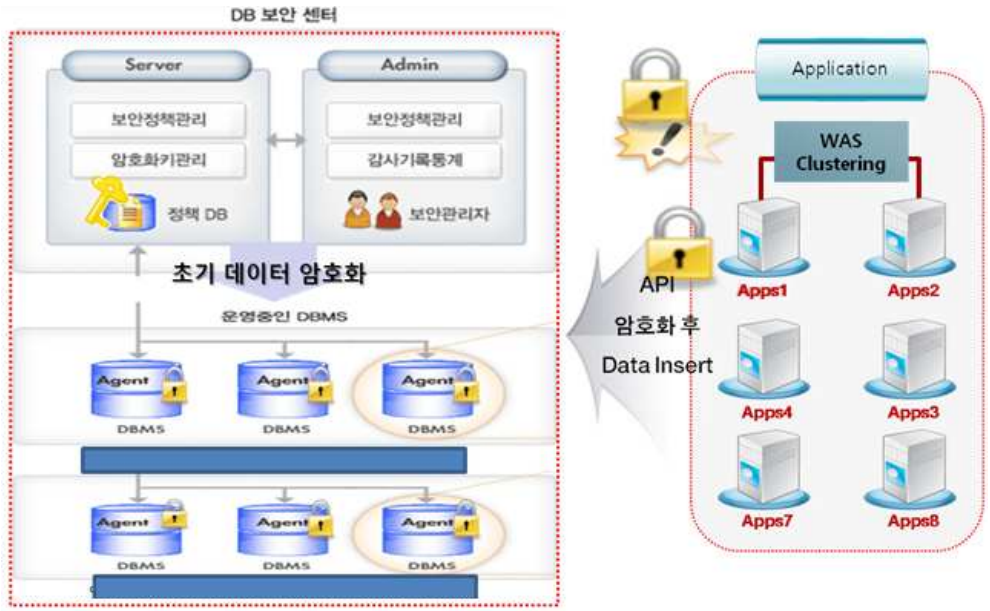
❍ 적용 환경

- 적용분야: 공공기관
- 업무종류: OO기관 대국민서비스
- 개인정보보유량: 약 9천3백만 건

❍ 적용 사유

- 차세대 시스템으로 새로운 응용프로그램 개발이 필요함
- 기존 DBMS에서 플러그인을 제공하지 않음

❍ 적용 구성도



<그림 16> 응용프로그램 자체 암호화 방식의 적용 구성도

❍ 주요 특징

- 암·복호화 작업이 다수의 어플리케이션 서버로 부하 분산
- 암호화 컬럼 크기 증가에 따라 관련 응용프로그램 인터페이스의 변경이 필요
- 암호화 후 DB 서버의 성능 저하는 적으나, 일부 질의에서는 색인 처리 불가로 응용프로그램 코드의 변경이 요구
- 암호화 컬럼 크기 증가에 따른 DB 서버 디스크 및 주기억장치 증설 필요
- 암·복호화 작업 부하에 따라 자원 여유율이 매우 작은 응용 서버(예 : WAS)는 자원 증설이 요구

2.1.2 DB 서버 암호화 방식

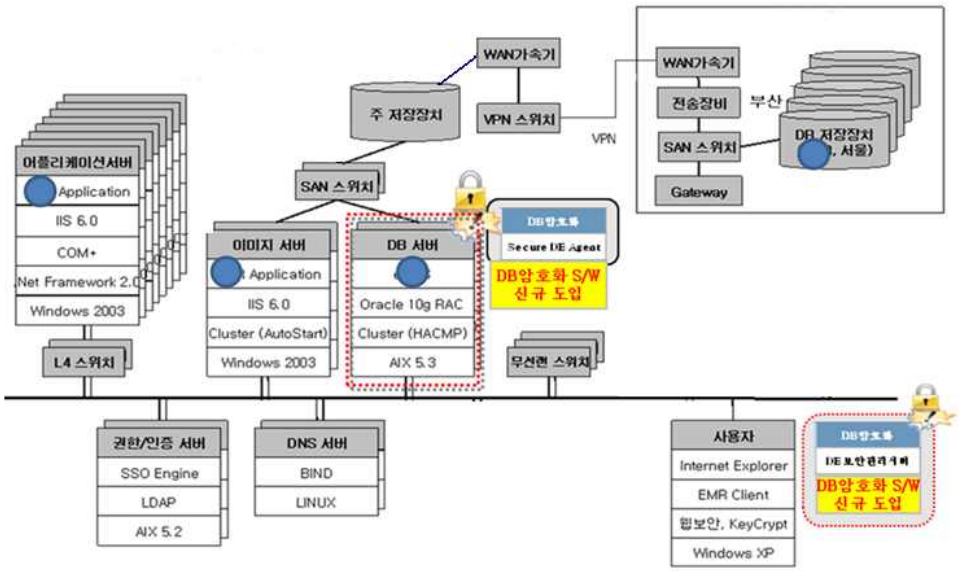
❍ 적용 환경

- 적용분야: 공공기관
- 업무종류: OO기관 통합정보시스템
- 개인정보보유량: 약 1억 건

❍ 적용 사유

- 운영 중인 응용프로그램 및 패키지 응용프로그램 수정을 최소화하여 단기간에 개발이 필요함
- 기존 DBMS에서 플러그인 기능을 제공함
- DB 서버의 성능 저하가 발생할 만한 복잡한 트랜잭션이나 배치 업무가 적음

❍ 적용 구성도



<그림 17> DB 서버 암호화 방식의 적용 구성도

❍ 주요 특징

- 암·복호화 작업이 DB 서버에 집중됨으로써 해당 서버의 자원 (CPU 및 주기억장치) 사용률 증가
- 암·복호화 뷰(암호화 이전 테이블명과 동일)와 트리거 구조를 이용하여 응용프로그램 변경 최소화
- 암호화 컬럼 크기 증가에 따라 관련 응용프로그램 인터페이스의 변경 필요
- 암호화로 인한 DB 성능 저하를 최소화하기 위하여 DB 질의와 응용프로그램의 튜닝 필요
- 암호화 컬럼 크기 증가와 암·복호화 작업 부하로 인해 DB 서버에 CPU 및 주기억장치, 디스크 증설 필요

2.1.3 DBMS 자체 암호화 방식

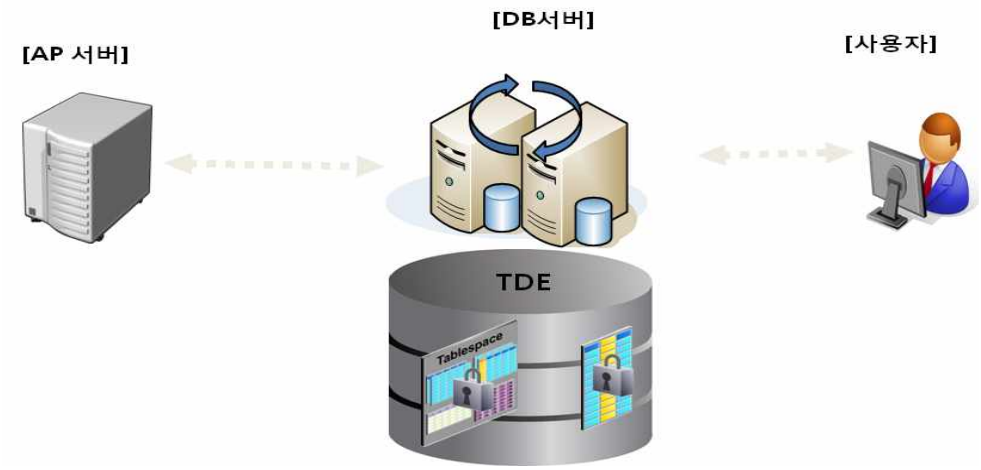
❍ 적용 환경

- 적용분야: 민간기관
- 업무종류: OO병원 수납시스템
- 개인정보보유량: 약 3억8천만 건

❍ 적용 사유

- 개발 인력의 부족으로 기존 응용프로그램의 수정을 최소화해야 함
- 대량 개인정보의 안정적인 처리가 필요함

❍ 적용 구성도



<그림 18> DBMS 자체 암호화 방식의 적용 구성도

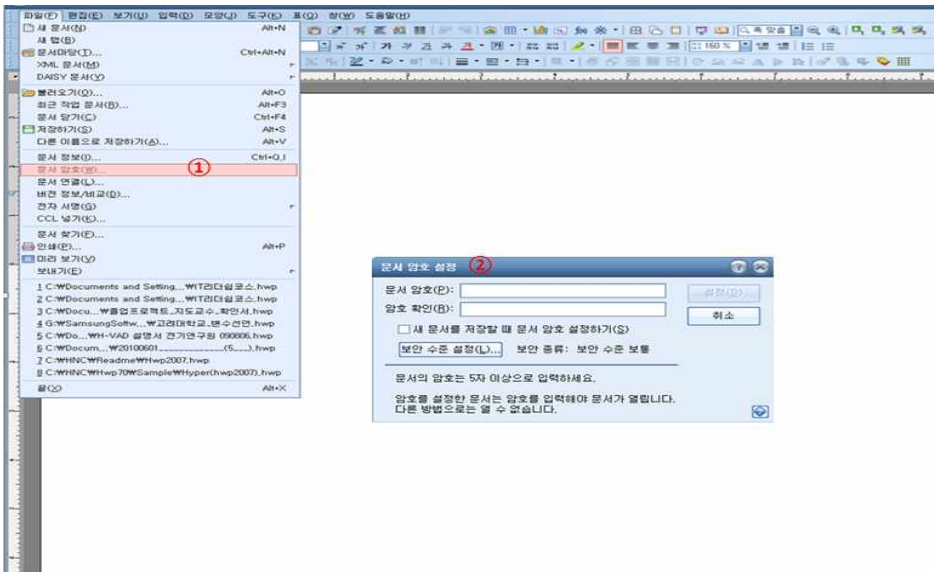
❍ 주요 특징

- DB 커널에서 암·복호화를 수행하므로 DB 서버의 CPU, 주기억장치, 디스크 등의 추가적인 부하가 적음
- 응용프로그램의 변경이 없으며, ERP 등 패키지에 암호화 적용 가능
- 암호화 테이블과 기존 테이블의 관리 도구 일원화로 운영 편의성 제공
- 비밀번호 일방향 암호화를 위한 암·복호화 모듈의 추가 필요

2.2 업무용 컴퓨터 암호화 사례

❍ 흔글 2007 문서 암호화 예제

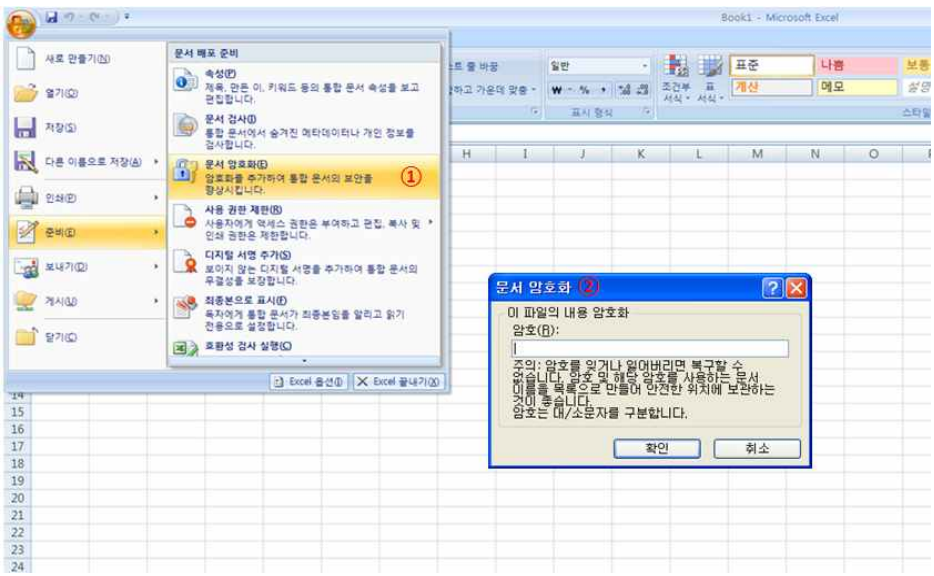
▪ [파일] → [문서암호] (흔글 2010의 경우: [보안] → [문서암호 설정])



<그림 19> 흔글 2007을 이용한 문서 암호화 적용

❍ MS 엑셀 2007 문서 암호화 예제

▪ [오피스 단추] → [준비] → [문서암호화] (MS 엑셀 2010의 경우 : [파일] → [정보] → [통합 문서 보호] → [암호 설정])



<그림 20> MS 엑셀 2007을 이용한 문서 암호화 적용

Ⅴ FAQ

【Q1】 공공기관이 아닌 일반기업입니다. 개인정보처리시스템의 DBMS (DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 고유식별정보 암호화시 안전한 알고리즘을 사용하도록 하고 있습니다. TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반 사항이 아닙니다.

【Q2】 공공기관입니다. 개인정보처리시스템의 DBMS(DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 암호화시 안전한 알고리즘을 사용하도록 하고 있으므로, TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반은 아닙니다.

다만, 공공기관은 전자정부법에 따라 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용하여야 합니다.

※ 자세한 사항은 "국가 정보보안 기본지침"을 확인하시기 바랍니다.

【Q3】 금융기관입니다. 개인정보처리시스템인 DBMS가 제공하는 TDE (Transparent Data Encryption) 방식을 사용한 암호화가 개인정보 보호법에 위배됩니까?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 암호화시 안전한 알고리즘을 사용하도록 하고 있으므로, TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반은 아닙니다.

다만, 전자금융감독규정에서 금융기관 또는 전자금융업자는 국가기관의 평가·인증을 받은 장비를 사용하도록 하고 있으므로 이를 확인하여야 합니다.

※ 자세한 사항은 "전자금융감독규정"을 확인하시기 바랍니다.

【Q4】 안전한 암호 알고리즘이 무엇인가요?

안전한 암호 알고리즘은 국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)에서 권고하고 있는 알고리즘을 의미합니다. 본 안내서의 '[표 1] 안전한 암호 알고리즘(예시)'를 참고하시기 바랍니다.

※ 공공기관은 IT보안인증사무국(http://service1.nis.go.kr)의 검증필 암호 모듈 또는 제품 참조

※ 암호기술 구현 안내서(2011.11, 한국인터넷진흥원). 암호 알고리즘 및 키 길이 이용 안내서(2009.3, · 한국인터넷진흥원)

【Q5】 주민등록번호를 저장하면 무조건 암호화해야 하나요?

인터넷에서 직접 접근이 가능한 구간(인터넷망, DMZ 구간)에 위치한 개인정보처리시스템에 주민등록번호를 저장하면 반드시 암호화해야 하며, 물리적인 망분리, 방화벽 등으로 분리된 내부망에 고유식별정보를 저장하는 경우에는 암호화 기술을 적용하거나 또는 암호화에 상응하는 조치를 할 수 있습니다.

※ '암호화에 상응하는 조치'란 「**개인정보 위험도 분석기준**」에 따라 보호조치를 이행하는 경우를 의미함 (개인정보 위험도 분석기준 및 해설서(행정안전부 공고 제2012-112)는 www.privacy.go.kr에서 다운로드)

【Q6】 DB에 저장된 주민등록번호를 일부분만 암호화해서 저장해도 되는 것인지요?

예, 일부분 암호화가 가능합니다. 시스템 운영이나 개인 식별을 위해 해당 정보를 활용해야 하는 경우 생년월일 및 성별을 포함한 앞 7자리를 제외하고 뒷자리 6개 번호를 암호화 하여 사용하실 수 있습니다.

(예:000000-1******)

【Q7】 DB에 외국인등록번호와 주민등록번호를 저장하고 있습니다. 둘 다 전체 암호화해서 저장해야 하나요?

외국인등록번호만 저장하는 경우에는 전체 암호화해야합니다. 외국인등록번호와 주민등록번호가 혼재되어 저장하는 경우에는 외국인등록번호 뒷부분 6자리만 암호화해도 무방합니다.

【Q8】 안전한 알고리즘이 다양한 키 길이를 제공하고 있는데, 키 길이에 상관없이 아무거나 사용해도 되나요?

암호 알고리즘은 키 길이 등에 따른 안전성 유지기간을 가지고 있으므로, 키 길이가 128 비트 미만인 대칭키 암호화 알고리즘과 해쉬값 길이가 112 비트 이하의 일방향 암호 알고리즘은 사용하지 않도록 권고합니다.

【Q9】 회사에 고객들의 이름, 주소, 전화번호, e-mail, 비밀번호를 저장하고 있습니다. 암호화 대상이 무엇인가요?

개인정보의 안전성 확보조치 기준 고시 제7조에서 암호화 대상은 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보입니다. 따라서 이 경우에는 비밀번호만 일방향 암호화해서 저장하시면 됩니다.

【Q10】 부동산중개업을 하고 있습니다. 업무용 컴퓨터에 ㅎ글, 엑셀을 이용하여 주민등록번호를 처리하고 있습니다. 암호화를 어떻게 해야 합니까?

ㅎ글, 엑셀 등을 이용하여 주민등록번호를 처리하는 경우 해당 프로그램에서 제공하는 비밀번호 설정 기능을 사용하여 암호화를 적용하시면 됩니다.

※ 업무용 프로그램에서 제공하는 비밀번호를 사용하는 경우 해당 프로그램에서 제공하는 암호화 알고리즘의 안전성을 확인하시기 바랍니다.

【Q11】 개인정보처리시스템을 위탁하거나, ASP(Application Service Provider)를 이용하는 경우 암호 수행을 위탁기관에서 해야 하는지 아니면 수탁기관에서 해야 하는지?

개인정보의 암호화 등 안전성확보조치는 원칙적으로 "개인정보처리자"의 의무입니다. 따라서 개인정보처리시스템을 위탁하거나 ASP를 이용하는 경우에도 암호화 조치사항에 대한 이행여부에 대한 책임은 위탁기관이 지게 됩니다.

다만, 위탁기관은 암호화에 대한 요구사항을 수탁기관과의 계약서 등에 명시하여 수탁기관으로 하여금 처리하게 요구할 수 있습니다.

[붙임 1] 국가정보원(IT보안인증사무국) 검증대상 암호알고리즘 목록

분류		암호알고리즘	참조표준
블록암호		ARIA SEED	KS X 1213-1(2009) KS X 1213-2(2009) TTAS.KO-12.0004/R1(2005) TTAS.KO-12.0025(2003)
해쉬함수		SHA-224 SHA-256 SHA-384 SHA-512	ISO/IEC 10118-3(2004) ISO/IEC 10118-3 Amd1(2006)
메시지 인증코드	해쉬함수 기반	HMAC	ISO/IEC 9797-2(2011)
	블록암호 기반	GCM(GMAC) CCM, CMAC	KS X 1213-2(2009) ISO/IEC 9797-1(2011) TTAK.KO-12.0131(2010)
난수발생기	해쉬함수/ HMAC기반	Hash_DRBG HMAC_DRBG	ISO/IEC 18031(2011) NIST SP 800-90
	블록암호 기반	CTR_DRBG	
키 설정 방식		DH ECDH	ISO/IEC 11770-3(2008) NIST FIPS 186-3
공개키 암호		RSAES	ISO/IEC 18033-2(2006)
전자서명		RSA-PSS, KCDSA, ECDSA, EC-KCDSA	ISO/IEC 14888-2(2008) ISO/IEC 14888-3(2006) TTAS.KO-12.0001/R1(2000) TTAS.KO-12.0015(2001) NIST FIPS 186-3

[붙임 2] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

□ 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

제7조(개인정보의 암호화)

① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 제3항, 제4항 및 제5항에 따른 개인정보 저장시 암호화를 적용하는 경우, 이 기준 시행일로부터 3개월 이내에 다음 각 호의 사항을 포함하는 암호화 계획을 수립하고, 2012년 12월 31일까지 암호화를 적용하여야 한다. 단 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다.

1. 개인정보의 저장 현황분석
2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법
3. 암호화 추진 일정 등

⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

□ 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화) 해설

> ① 영 제21조 및 영 제30조에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

■ "고유식별정보"는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며, 대통령령으로 주민등록번호, 여권번호, 면허번호, 외국인등록번호 등을 정하고 있다.

■ "비밀번호"는 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

■ "바이오정보"는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

> ② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

■ 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보 등 정보통신망 내외부로 송·수신할 모든 개인정보에 대해서는 암호화하여야 한다.

· 내부망 내에서 송·수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화하여야 한다.
· 전용선을 이용하여 개인정보를 송·수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등을 대비해서 가급적 암호화 전송을 권장한다.

■ 개인정보 암호화 전송을 위해 보안서버를 활용할 수 있다.

· "보안서버"란 웹서버에 SSL(Secure Sockets Layer) 인증서나 암호화 소프트웨어를 설치하여 암호통신을 수행하는 방식을 말한다.

■■■ 보안서버 구축방식 예시 ■■■

〈SSL 방식의 보안서버 실행 확인〉

〈응용프로그램 방식의 보안서버 실행 확인〉

■ "보조저장매체"는 컴퓨터에 장착된 하드디스크(HDD) 등의 저장매체 이외에 전자적으로 자료를 저장할 수 있는 매체로서 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓, 자기 테이프 등 개인정보처리시스템, 업무용 컴퓨터 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

- 이러한 매체에 개인정보를 저장 후 분실할 경우, 개인정보가 노출될 위험이 있으므로, 암호화 기능을 제공하는 보조저장매체를 사용하거나 개인정보를 암호화 저장하여 분실되더라도 다른 사람이 알 수 없도록 조치하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

■ 개인정보처리자는 비밀번호, 바이오정보(지문, 홍채 등)가 노출 또는 위·변조되지 않도록 암호화 하여 저장하여야 하며, 특히 비밀번호의 경우에는 복호화되지 않도록 일방향 (해쉬함수) 암호화 하여야한다.

■ 일방향 암호화는 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.

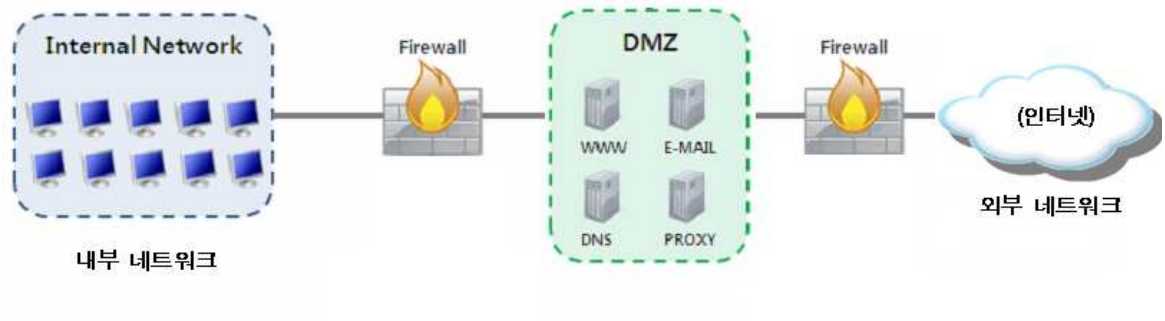
■■■ 일방향(해쉬 함수) 암호화 ■■■

- 일방향(해쉬 함수) 암호화는 입력된 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 길이가 고정된 결과를 만들어 내는 방법을 의미한다.
- 일방향(해쉬 함수) 암호화의 가장 기본적인 성질은 두 해쉬 결과가 다르다면 원래의 데이터도 어딘가 다르다는 것을 의미하며, 원래 입력의 한 비트만 바뀌더라도 해쉬 결과는 크게 달라지기 때문에 전자서명 방식에 이용되고 있다.

■ 바이오 정보의 경우, 복호화가 가능한 양방향 암호화 저장이 필요하나, 이는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외된다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

■ 인터넷 구간은 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간, DMZ 구간은 인터넷과 내부망과 인터넷 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말한다. 내부망은 접근통제시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말한다.



■ 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 이에 따라 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제2항에 따른 비밀번호 및 바이오 정보를 저장하는 경우에도 암호화하여 저장해야한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 결정할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

■ 내부망에 고유식별정보를 저장하는 경우, 개인정보 영향평가 및 위험도 분석 결과에 따라 암호화 적용여부 및 적용범위를 결정하여 시행할 수 있다.

- 영 제35조에 따라 영향평가의 대상이 되는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정한다.
- 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행한다.

· 개인정보 영향평가 수행을 위한 교육교재 참조

■ "위험도 분석"은 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

- 세부적으로 위험도 분석은 개인정보 유출에 영향을 미칠 수 있는 다양한 위협에 대한 시스템 취약점과 이로 인해서 예상되는 손실을 분석하여 위험요소를 식별, 평가하고 그러한 위험요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 위험관리의 일부분이다.

■ "위험도 분석"은 개인정보를 저장하는 정보시스템에서 개인정보파일 단위로 수행하고 각 개별 개인정보파일의 위험점수에 따라 개별 개인정보파일 단위로 암호화 여부를 결정해야하며, 위험도 분석을 수행한 결과는 최고경영층으로부터 내부결재 등의 승인을 받아야 한다.

· 위험도 분석 점검표 참조

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

■ "안전한 암호 알고리즘"이란 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 및 국내외 암호 연구기관에서 권고하는 알고리즘을 의미한다.

· 고유식별정보, 바이오 정보는 원칙적으로 암호화해야 하나, 시스템 운영이나 개인 식별을 위해 해당 개인정보를 활용하는 경우 암호화/복호화에 대한 부하가 발생할 수 있다. 이 경우, 주민등록번호 등과 매핑하여 임의의 서비스 번호를 부여해서 사용할 수 있으며 임의의 서비스번호와 매핑되는 주민등록번호는 암호화하여 저장·관리하여야 한다.

■ 주민등록번호를 시스템 운영을 위한 검색 키로 사용하는 경우, 속도 등 성능을 고려하여 일부 정보만 암호화 조치를 취할 수 있다.

※ 주민등록번호의 경우 뒷자리 6개 번호 이상 암호화 조치 필요(예시: 700101-1#……&)

⑦ 개인정보처리자는 제3항, 제4항 및 제5항에 따른 개인정보 저장시 암호화를 적용하는 경우, 이 기준 시행일로부터 3개월 이내에 다음 각 호의 사항을 포함하는 암호화 계획을 수립하고, 2012년 12월 31일까지 암호화를 적용하여야 한다. 단 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다.

1. 개인정보의 저장 현황분석
2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법
3. 암호화 추진 일정 등

■ 개인정보처리자가 고유식별번호, 비밀번호, 바이오 정보를 처리하는 경우, 제3항, 제4항 및 제5항에서 규정한 암호화 시행을 위해, 조직 내 의사결정권자의 승인을 득한 암호화 계획을 수립하여 2012년 12월 31일까지 적용하여야 한다.

■■■ 암호화 계획 주요내용 ■■■

1. 개인정보의 저장 현황분석

· 비밀번호, 바이오정보, 고유식별정보를 저장하는 경우에는 암호화의 대상이 되므로 암호화 방법을 결정하기 위해, 개인정보처리자는 제공하는 각 서비스별로 저장하는 개인정보의 종류, 규모, 보유·이용 기간 등의 현황과 이들 서비스를 위해 처리되는 개인정보 보호를 위한 관리적·기술적 보호조치 현황을 분석하여야 한다.

2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법

· 개인정보 영향평가 실시 대상에 따라 개인정보 영향평가를 실시해야 하는 경우에는 영향평가 절차 및 방법을 그 외에 공공기관이나 개인정보처리자는 위험도 분석 절차 및 방법을 작성하여야 한다.
※ 영향평가·위험도 분석 절차 및 방법은 본 기준의 제7조 5항 참조

3. 암호화 추진 일정 등

· 영향평가·위험분석 시행시기 및 암호화 구축 시기 등을 포함한 세부 추진 일정 등을 작성하여야 한다.

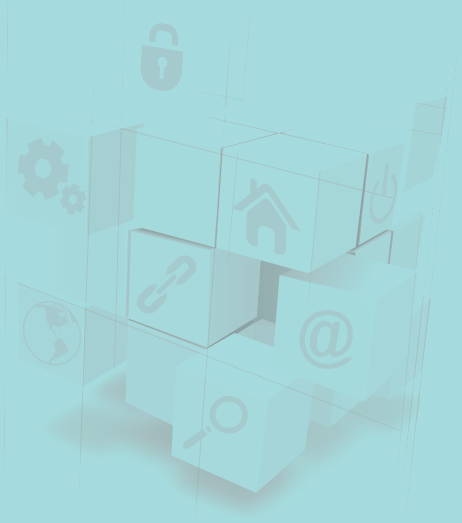
· 법 시행 이후 주민등록번호 등 암호화 대상이 포함된 개인정보를 개인정보처리시스템을 신규로 구축하는 경우, 암호화를 즉시 이행하여야 한다.

⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

■ 고유식별정보를 업무용 컴퓨터에 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려 받아 저장할 때는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다.

Ⅰ. 가이드라인 개요

제1절 **목적 및 개요**
제2절 **적용범위**
제3절 **가이드라인 구성**
제4절 **관련 법령 및 지침**
1. 관련법령
2. 관련지침



Ⅰ 가이드라인 개요

제1절 목적 및 개요

- 개인정보처리시스템 개발 · 구축과 관련하여 개인정보보호 관련 법령, 지침 및 규정 등에 위배되지 않도록 개발자 또는 운영자가 개인정보처리시스템의 기획, 개발 · 구축, 운영의 각 단계별로 준수하여야 하는 조치사항 제시
- 본 가이드라인에서는 현재 시행되고 있는 개인정보보호 관련 법령, 지침, 고시 등을 종합적으로 분석하여 개인정보처리시스템을 기획, 개발 · 구축, 운영 단계에서 준수 또는 고려하여야 할 사항에 대하여 제시

제2절 적용범위

- 개인정보처리시스템을 기획, 개발 · 구축, 운영하려는 모든 개발자 및 운영자를 대상으로 적용
- 본 가이드라인은『개인정보 보호법』을 기준으로 작성하였으며, 정보통신사업자에 해당하는 경우 업무에 참조할 수 있도록 『정보통신망법』 등을 별도로 추가하여 언급

제3절 가이드라인 구성

1. 전체구성

제1장 가이드라인 개요

본 가이드에 대한 전반적인 이해를 도울 수 있도록 가이드라인의 목적, 적용범위 및 구성형식 등 소개

제2장 개인정보처리시스템 기획 단계

시스템 개발의 기획단계에서 시스템 개발자 및 운영자가 개인정보보호를 위하여 고려하여야 하는 조치사항

제3장 개인정보처리시스템 개발 · 구축 단계

개인정보처리시스템의 개발 · 구축 단계에서 개인정보보호를 위하여 고려하여야 하는 조치사항

제4장 개인정보처리시스템 운영 단계

개인정보처리시스템의 운영 단계에서 적용하여야 하는 개인정보보호를 위한 운영관리 및 보안관리 방안

2. 가이드라인 구성형식

본 가이드라인의 각 장은 다음과 같은 형식으로 구성되어 있음

- 목적 및 개요 : 각 장의 목적 및 개요
- 적용범위 : 실제 적용되는 범위에 대해 요약
- 기본원칙 : 반드시 숙지해야 할 기본적인 법령, 지침 등
- 준수사항 : 정보보안 및 개인정보보호를 위한 각 분야별 조치사항
- 참조문서 : 각 장에서 기술한 내용을 위해 참조한 문서 요약

제4절 관련 법령 및 지침

1. 관련법령

- 개인정보 보호법
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 정보통신기반 보호법
- 위치정보의 보호 및 이용 등에 관한 법률
- 전기통신사업법
- 전자서명법

2. 관련지침

- 개인정보의 안전성 확보조치 기준(행정자치부고시, 제2014-7호)
- 표준 개인정보 보호지침(행정안전부고시, 제2011-45호)
- 개인정보 영향평가에 관한 고시(행정안전부고시, 제2012-59호)
- 개인정보의 기술적 · 관리적 보호조치 기준(방송통신위원회고시, 제2012-50호)
- 주요정보통신기반시설 취약점 분석 · 평가 기준(미래창조과학부고시, 제2013-37호)

Ⅱ. 개인정보처리시스템 기획 단계

제1절 **목적 및 개요**
제2절 **적용범위**
제3절 **기본원칙**
제4절 **준수사항**
1. 개인정보보호 관련 법령 및 지침 검토
2. 개인정보 수집 최소화를 위한 방안 마련
3. 개인정보 파기 방안 마련
4. 주민등록번호 이외 회원가입 방안 마련
5. 개인정보처리시스템에 대한 보안 대책 마련
6. 개인정보 저장 및 전송 시 암호화 방식 결정
7. 개인정보 처리(취급)방침 수립
8. 개인정보 영향평가 고려사항
9. 시큐어 코딩을 적용한 개발 방안 마련
제5절 **참고문서**

Ⅱ 개인정보처리시스템 기획 단계

제1절 목적 및 개요

- 본 장은 개인정보처리시스템을 도입하기 전 기획 단계에서 개인정보보호를 위해 필요한 각종 요소들을 사전에 식별하여 반영하기 위해 관련 법령 등을 검토하고 관련 법령에서 요구하고 있는 필요 최소한의 요건을 만족하기 위해 필요한 내용을 제시한다.

제2절 적용범위

- 개인정보처리시스템을 기획하는 단계에서 개발자 및 운영자가 준수하여야 할 사항을 다루고 있다.

제3절 기본원칙

개인정보처리시스템을 기획하는 단계에서 개인정보보호를 위해 검토하고 확인하여야 할 기본원칙은 아래와 같다.

- 개인정보보호 관련 법령 및 지침 등 관련 규정을 세부적으로 검토
- 개인정보 수집 최소화를 위해 개인정보 처리 목적을 명확히 하고 수집
- 개인정보 목적 달성 시 파기 방법을 사전에 결정
- 주민등록번호 이외 추가 인증수단을 통한 회원가입 방법 제공
- 개인정보처리시스템에 대한 접근권한 등 기본적인 보안대책 마련
- 개인정보 전송 및 저장 시 적용할 암호화 알고리즘과 방식 결정
- 개인정보처리시스템과 관련된 개인정보 처리(취급)방침 수립
- 공공기관 개인정보처리시스템과 관련하여서는 개인정보 영향평가 고려
- 개발단계에서 적용해야 할 시큐어 코딩에 대한 기준 정의

제4절 준수사항

1. 개인정보보호 관련 법령 및 지침 검토

개인정보처리시스템 개발 · 구축에 앞서 사업담당자 및 개발자는 개인정보보호와 관련된 법령 및 지침 등을 반드시 검토하여 이를 시스템 개발 · 구축시 반영하여야 한다.

관련근거

① 개인정보 보호법 제1조(목적), 제6조(다른 법률과의 관계)
② 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4장 개인정보의 보호

법령 및 고시는 반드시 준수해야 하는 최소한의 의무사항이다. 그러므로 아래와 같은 개인정보보호 관련 법령 및 고시 등의 최신 내용을 반드시 검토하여 적용하여야 한다.

개인정보보호 관련 법령을 적용함에 있어서 다른 법률에 특별한 규정이 있는 경우를 제외하고는 『개인정보 보호법』에서 정하는 바에 따른다.

[표 1] 개인정보보호 관련 법령 및 고시

구분	명칭
법령	개인정보 보호법
	정보통신망 이용촉진 및 정보보호 등에 관한 법률
	전자정부법
	정보통신기반 보호법
	위치정보의 보호 및 이용 등에 관한 법률
	신용정보의 이용 및 보호에 관한 법률
고시	개인정보의 안전성 확보조치 기준(행정자치부 고시, 제2014-7호)
	표준 개인정보 보호지침(행정안전부 고시, 제2011-45호)
	개인정보 영향평가에 관한 고시(행정안전부 고시, 제2012-59호)
	개인정보의 기술적 · 관리적 보호조치 기준(방송통신위원회 고시, 제2012-50호)

개인정보보호 관련 규정을 위반한 경우 처벌과 관련된 사항은 [별첨 1]『개인정보보호 관련 규정 위반 시 처벌(개인정보 보호법 기준)』과 [별첨 2]『개인정보보호 관련 규정 위반 시 처벌(정보통신망법 기준)』을 참고한다.

[표 2] 개인정보보호 관련 검토 및 참고사항

구분	명칭	위치
개인정보 처리방침	개인정보처리방침 만들기	http://www.privacy.go.kr/a3sc/per/inf/perInfStep01.do
주민번호 대체수단	인터넷 사업자를 위한 주민번호 사용 제한 정책, 준비 안내서	https://www.i-privacy.kr/servlet/command.user.board.BoardCommand?select_cat1=4&select_cat2=4
	i-PIN 2.0 도입 안내서	
	i-PIN을 이용한 회원가입 사례	http://i-pin.kisa.or.kr/kor/use/example.jsp
웹서버 구축보안	웹서버 구축 보안점검 안내서	http://www.kisa.or.kr/public/laws/laws3.jsp
	웹어플리케이션 보안 안내서	
	홈페이지 개발보안 안내서	

구분	명칭	위치
웹서버 구축보안	WebKnight를 활용한 IIS 웹서버 보안 강화 안내서	http://www.kisa.or.kr/public/laws/laws3.jsp
	ModSecurity를 활용한 아파치 웹서버 보안 강화 안내서	
	보안서버 구축 안내서	
패스워드 및 암호화	패스워드 선택 및 이용 안내서	http://www.kisa.or.kr/public/laws/laws3.jsp
	암호이용 안내서	
	암호 알고리즘 및 키 길이 이용 안내서	
	암호정책 수립 기준 안내서	
	암호기술 구현 안내서	
취약점 진단	홈페이지 취약점 진단제거 가이드	http://www.kisa.or.kr/public/laws/laws3.jsp
	웹 취약점 점검	http://www.privacy.go.kr/a3sc/per/tec/check/tecSupportCheck.do
	업무용 PC 보호조치 점검도구 신청	http://www.privacy.go.kr/a3sc/per/tec/chk/checkToolReq.do
개인정보 영향평가	기업의 개인정보영향평가 수행을 위한 안내서	http://www.kisa.or.kr/public/laws/laws3.jsp
	사업자를 위한 개인정보 영향평가	http://www.privacy.go.kr/per/iass/info/evalInfo.do
시큐어코딩	소프트웨어 개발 보안 가이드	http://www.kisa.or.kr/public/laws/laws3.jsp
	JAVA 시큐어코딩 가이드	
	C 시큐어코딩 가이드	
	Android-JAVA 시큐어코딩 가이드	
	소프트웨어 보안약점 진단가이드	
기타	웹사이트 회원탈퇴 기능 구현 안내서	http://www.kisa.or.kr/public/laws/laws3.jsp
	백신 프로그램 이용 안내서	
	사업자 필수 조치사항	http://www.privacy.go.kr/nns/ntc/cor/personalImportant2.do
	개인정보 보호조치 가이드	http://www.privacy.go.kr/per/rel/dev/Guide.do
	페이스북 이용자를 위한 개인정보보호 안내서	https://www.i-privacy.kr/servlet/command.user.board.BoardCommand?select_cat1=4&select_cat2=4
	개정 정보통신망법 개인정보보호 신규제도 안내서	
	앱 개발자를 위한 개인정보보호 안내서	

2. 개인정보 수집 최소화를 위한 방안 마련

이용자의 개인정보를 수집하는 경우 서비스의 제공을 위하여 필요한 최소한의 정보만을 수집하여야 하며, 필요한 최소한의 정보 이외에 개인정보를 제공하지 아니한다는 이유로 그 서비스 제공을 거부하여서는 안 된다.

관련근거

① 개인정보 보호법 제16조(개인정보의 수집 제한)
② 정보통신망법 제23조2(개인정보 수집 제한 등)

개인정보 수집을 최소화하기 위해서는 개인정보처리시스템을 개발하기에 앞서 개인정보처리시스템에서 처리하는 개인정보에 대한 명확한 목적을 먼저 정의해야 한다.

[표 2] 개인정보보호 관련 검토 및 참고사항

주의사항

① 서비스를 제공하는 데 있어 필요한 이용자의 개인정보가 무엇이 있는지 그 종류를 조사한다.
② 조사한 개인정보 중 필수적으로 수집해야하는 “필수 동의 항목”을 검토하여 구성한다.
③ 필수/선택 동의 사항을 명시적으로 구분하여 수집한다.

개인정보 수집 시에는 필요 최소한의 개인정보만을 수집해야 하며, 이 때 아래와 같은 『필수 동의 항목과 선택 동의 항목의 구분 예시』를 참고하여 불필요한 개인정보가 수집되지 않도록 하여야 한다. 아울러 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스 제공을 거부할 수 없다.

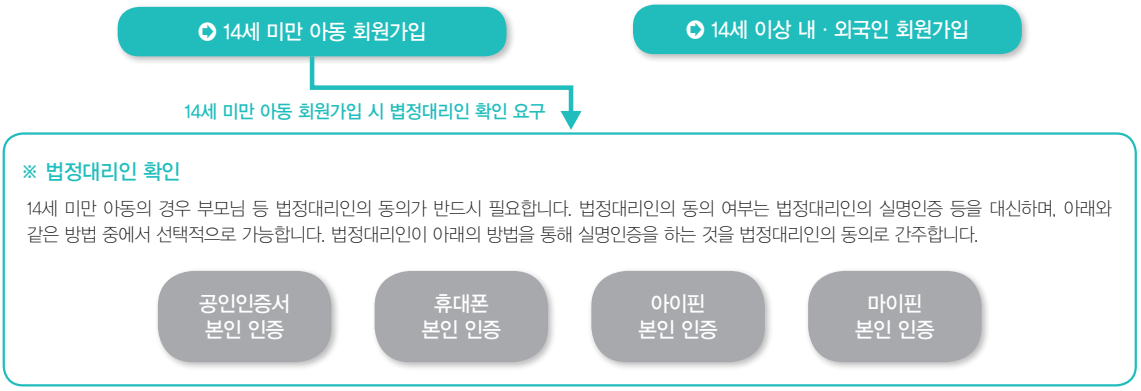
[표 3] 필수 동의 항목과 선택 동의 항목의 구분 예시

<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>정의</td><td>• 필수 동의 항목은 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보
– 본질적 기능은 사업자가 해당 서비스 제공 과정에서 업무처리에 반드시 필요한 기능
– 이용자에게 필수적 동의 요구 가능
– 이용자가 필수 동의 항목에 동의하지 않으면 서비스를 제공 받을 수 없음

• 선택 동의 항목은 사업자의 필요에 의하거나 추가적인 서비스를 위해 필요한 정보
– 이용자가 동의 여부 선택 가능
– 사업자는 선택 동의 항목에 동의하지 않는다고 해서 서비스 이용을 거부해서는 안 됨</td></tr>
<tr><td>예시</td><td>※ 아래는 필수/선택 동의 항목의 예시임

① 인터넷 회원제 서비스
<table>
<tr><th>구분</th><th>필수 동의</th><th>선택 동의</th></tr>
<tr><td>목적</td><td>회원의 신원 확인 및 관리</td><td>상품 등에 대한 홍보 및 마케팅</td></tr>
<tr><td>수집 항목</td><td>아이디, 비밀번호, 이름, 이메일</td><td>휴대전화번호, 생년월일, 성별, 결혼여부, 사용자 선호도 등</td></tr>
</table>
② 온라인 결제 서비스
<table>
<tr><th>구분</th><th>필수 동의</th><th>선택 동의</th></tr>
<tr><td>목적</td><td>안전한 온라인 결제</td><td>결제 알림 서비스</td></tr>
<tr><td>수집 항목</td><td>결제정보(카드번호, 계좌번호 등), IP, MAC, 휴대폰 기기 정보 등 사용 기기에 관련한 정보</td><td>휴대폰번호, 이메일 주소 등</td></tr>
</table>
③ 이동통신 서비스
<table>
<tr><th>구분</th><th>필수 동의</th><th>선택 동의</th></tr>
<tr><td>목적</td><td>휴대전화 이용</td><td>멤버쉽 할인</td></tr>
<tr><td>수집 항목</td><td>신청인(또는 법정 대리인)의 성명, 주소, 연락전화번호, 요금 납부자의 성명, 생년월일, 계좌 정보, 신청인과의 관계 등</td><td>멤버쉽 카드 정보, 멤버쉽 ID, 고객 등급, 생일, 성별 등</td></tr>
</table></td></tr>
<tr><td>14세미만 아동</td><td>14세 미만 아동 개인정보 처리시 법정대리인의 동의 필요
법정대리인의 동의를 받기 위해서 필요한 최소한의 정보(연락처)는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집 가능</td></tr>
</table>

개인정보처리시스템에서 14세 미만 아동에 대한 개인정보 수집이 필요한 경우에는 일반회원과 구분하여 아래 그림과 같이 처리할 수 있다.



[그림 2] 14세 미만 아동 회원가입 시 법정대리인 동의

행정처분 사례

● 개인정보 수집 시 필요 최소한 수집 · 과도한 수집 금지 위반 사례

제16조제1항 위반 : 시정조치 또는 개선권고

- 홈페이지 회원정보 수집 후 준영구 보유(→ 이용 및 보유기간을 수집 목적에 맞게 조정 필요)
- 민원처리, 수수료 정산 명분으로 개인정보를 과도 수집 · 보관
- 수취인 확인의 유일 정보로 보기 어려운 지문정보까지 과도 수집
- 열람 청구에 따른 정당한 정보주체 또는 대리인 여부 확인 시 신분증 복사 등 과도한 개인정보 수집

● 최소한의 정보 외의 수집에 미동의 시 재화 또는 서비스 제공 거부 금지 위반 사례

제16조제2항 위반 : 3천만원 이하의 과태료(1회 위반 600만원)

- 홈페이지에서 선택정보인 주소 수집에 미동의 시 회원가입 절차가 정지되어 서비스 이용 제한됨

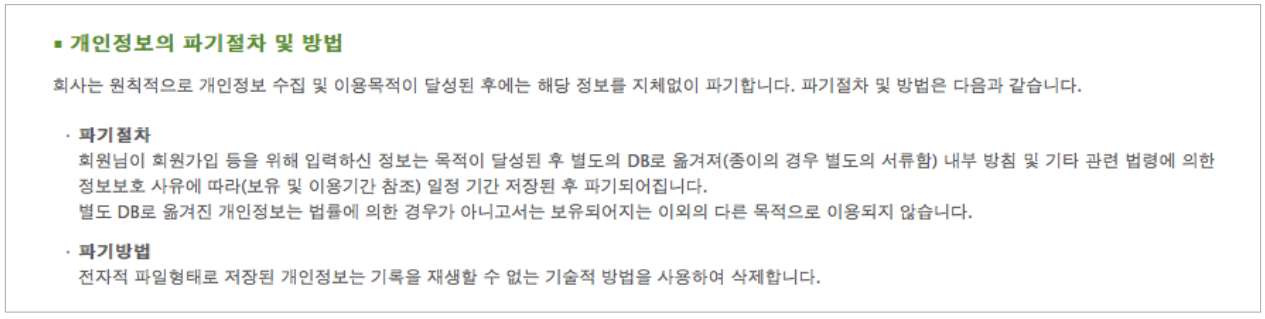
3. 개인정보 파기 방안 마련

개인정보의 수집 목적 달성 및 이용기간의 종료, 또는 폐업하는 경우에는 보유하고 있는 개인정보를 지체하지 않고 파기해야 한다. 이에 따라 개인정보처리시스템을 기획하는 단계에서부터 개인정보 파기에 대한 방안을 마련해야 한다.

관련근거

① 개인정보 보호법 제21조(개인정보의 파기)
② 정보통신망법 제29조(개인정보의 파기)

회원가입을 통해 정보주체의 개인정보를 수집할 때에는 회원가입 시 회원탈퇴 방법을 정보주체가 알기 쉽도록 알려야 한다. 이에 대한 예시로는 회원탈퇴를 신청 할 수 있는 메뉴를 눈에 띄게 설정하거나 개인정보처리 담당자의 연락처를 이용자가 찾기 쉬운 곳에 공지하는 방법이 있다.



▪ 개인정보의 파기절차 및 방법

회사는 원칙적으로 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체없이 파기합니다. 파기절차 및 방법은 다음과 같습니다.

· 파기절차
회원님이 회원가입 등을 위해 입력하신 정보는 목적이 달성된 후 별도의 DB로 옮겨져(종이의 경우 별도의 서류함) 내부 방침 및 기타 관련 법령에 의한 정보보호 사유에 따라(보유 및 이용기간 참조) 일정 기간 저장된 후 파기되어집니다.
별도 DB로 옮겨진 개인정보는 법률에 의한 경우가 아니고서는 보유되어지는 이외의 다른 목적으로 이용되지 않습니다.

· 파기방법
전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제합니다.

[그림 3] 개인정보의 파기절차 및 방법 안내 예시

파기 사유가 발생한 경우, '복구 · 재생할 수 없는 방법'으로 파기해야 한다. 파기와 관련된 구체적인 시기와 방법 등에 관한 사항은 제4장 개인정보처리시스템 운영 단계에 포함된 '개인정보 파기 시 조치사항' 항목을 참조한다.

행정처분 사례

- 보유기간 경과, 처리목적 달성 후 개인정보 미파기 위반사례

제21조제1항 위반 : 3천만원 이하의 과태료(1회 위반 600만원)

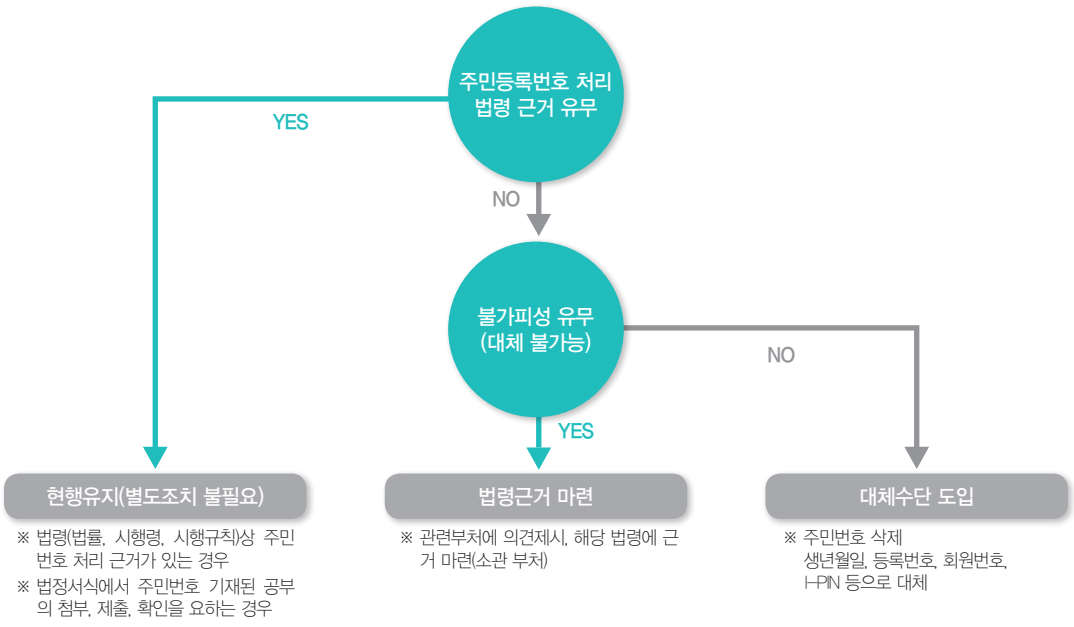
- 홈페이지에서 탈퇴한 회원정보 일부 또는 전부 미파기
- 보유기간을 경과하거나 수집목적을 달성한 개인정보 미파기
- 보존기간이 경과된 개인정보(이름/연락처/성별) 미파기

4. 주민등록번호 이외 회원가입 방안 마련

개인정보의 수집 목적 달성 및 이용기간의 종료, 또는 폐업하는 경우에는 보유하고 있는 개인정보를 지체하지 않고 파기해야 한다. 이에 따라 개인정보처리시스템을 기획하는 단계에서부터 개인정보 파기에 대한 방안을 마련해야 한다.

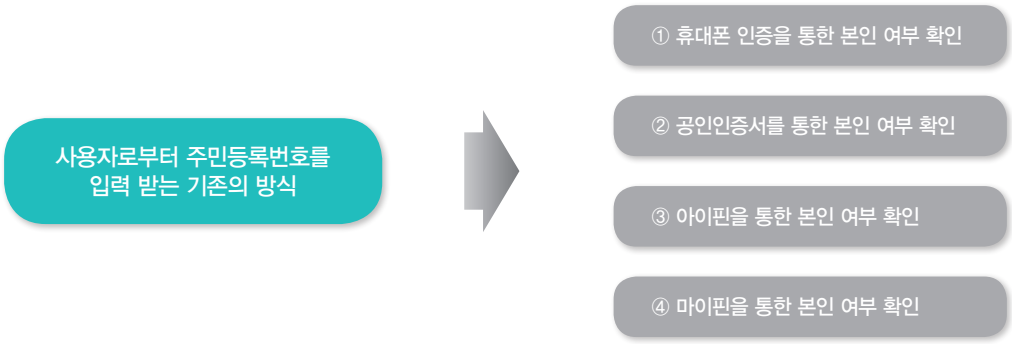
관련근거

① 개인정보 보호법 제24조의2(주민등록번호 처리의 제한)
② 정보통신망법 제23조의2(주민등록번호의 사용 제한)



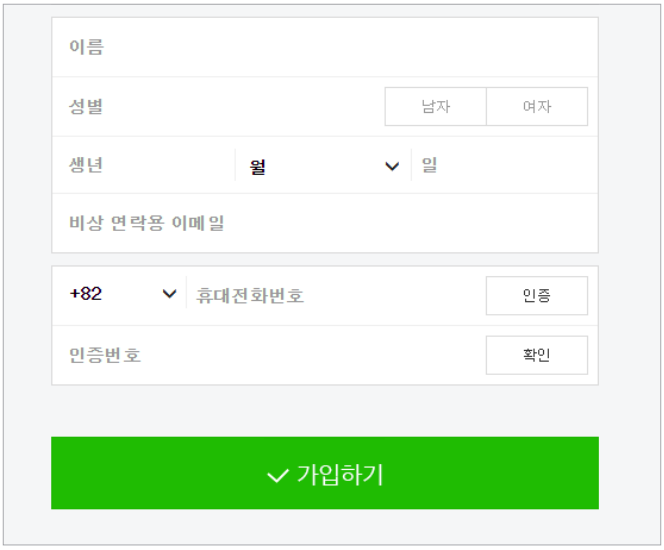
[그림 4] 주민등록번호 수집 금지 제도 가이드라인(행정자치부, 2014.1)

법령에서 구체적으로 주민등록번호 처리 근거가 있는 경우를 제외하고 주민등록번호를 수집할 수 없다. 본인 여부를 확인해야 하는 경우에는 아래와 같이 주민등록번호 이외의 대체수단을 이용해야 한다.



[그림 5] 주민등록번호 대체 수단

❶ 휴대폰 인증을 통한 본인 여부 확인



[그림 6] 휴대폰 인증 적용 예시

휴대폰을 통한 본인 인증은 이용자의 휴대전화번호와 간단한 인적사항을 이용하는 방법으로 통신사를 통해 본인 명의로 휴대폰을 발급 받아 이용하는 사용자를 대상으로 하며, 인증을 시도하는 경우 인증 서비스 업체에서 발송하는 SMS 인증번호 확인을 통해 본인 여부를 인증한다.

이를 도입하는 방법 및 절차는 사업자의 업종 및 규모에 따라 달라질 수 있으므로 휴대폰 인증을 제공하는 본인확인기관에 연락하여 자세한 정보 및 해당 시스템 도입에 따른 사항을 상담 받도록 한다.

❷ 공인인증서 통한 본인 여부 확인

공인인증기관에서 발급받은 공인인증서로 본인 여부를 확인할 수 있다. 한국인터넷진흥원의 전자서명인증관리센터(www.rootca.or.kr)에서는 공인인증서 소프트웨어 구현과 관련하여 기술 가이드라인을 제공하고 있다.

[그림 7] 공인인증서 SW 구현

❸ 아이핀을 통한 본인 여부 확인

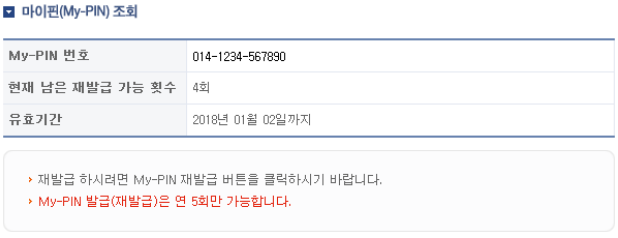
아이핀은 주민등록번호를 대신하여 아이디/패스워드로 신원을 확인할 수 있는 방법으로 민간 본인확인기관에서 도입 · 발급 · 운영하는 민간 아이핀과 행정자치부의 공공아이핀 센터에서 도입 · 발급 · 운영하는 공공아이핀으로 구분된다.

- 민간 아이핀: NICE아이핀(1588-2486), SIREN24(1577-1006)
- 공공 아이핀: 공공아이핀센터(02-818-3050)

❹ 마이핀을 통한 본인 여부 확인

마이핀은 행정자치부에서 2014년부터 시행하는 온/오프라인 본인확인수단이다.

- 행정자치부 : http://www.g-pin.go.kr/center/pic/sub_05.gpin
- 개인정보보호 종합지원 포털 : http://privacy.go.kr/file/MyPin_Q_A.pdf
- NICE평가정보 : https://www.vno.co.kr/ipin3/mypin_01.asp
- 서울신용평가정보 : http://www.siren24.com/index.jsp



[그림 8] 마이핀(My-PIN) 발급 조회 화면

5. 개인정보처리시스템에 대한 보안 대책 수립

정보주체의 개인정보를 안전하게 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위해 개인정보 보호책임자를 지정하고, 수집된 개인정보를 취급하는 자를 최소한으로 제한하여야 한다. 또한 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위해 기술적 · 관리적 · 물리적조치를 하여야 한다.

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

개인정보처리시스템에 보관된 개인정보는 지정된 관련 업무 담당자만 열람할 수 있도록 하고, 영업부서의 접근을 제한하여 외부 영업목적(텔레마케팅 등)으로 이용할 수 없도록 제한하여야 하며, 필요에 따라 최소한의 정보에만 접근할 수 있도록 하여야 한다.

주의사항

① 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립 및 시행
② 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치 및 운영
③ 접속기록의 위조 및 변조 방지를 위한 필요한 조치 방안 강구
④ 개인정보를 안전하게 저장 및 전송할 수 있는 암호화기술 등을 이용한 보안조치
⑤ 백신 소프트웨어의 설치 및 운영 등 컴퓨터바이러스에 의한 침해 방지 조치
⑥ 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 강구

개인정보처리자는 개인정보를 처리함에 있어 안전하게 처리하기 위해 아래와 같은 사항을 포함한 내부관리계획을 수립하고 이행하여야 한다.

주의사항

① 개인정보 보호책임자의 지정에 관한 사항
② 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
③ 개인정보의 안전성 확보에 필요한 조치에 관한 사항
④ 개인정보취급자에 대한 교육에 관한 사항
⑤ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
⑥ 그 밖에 개인정보 보호를 위하여 필요한 사항

※ 소상공인은 생략 가능

개인정보처리자는 수립된 내부관리계획의 내용 중에서 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.
개인정보처리시스템에 대한 관리자 페이지 등에 대한 접근통제를 위해서는 소프트웨어 또는 하드웨어 방식의 접근통제를 적용할 수 있으며, 이는 개인정보처리자가 적절히 판단하여 결정할 수 있다.
아래는 일반적인 접근통제의 방식으로, 접근통제시스템을 적용할 때 해당 방식별 특징 등을 잘 분석하여 가장 적합한 방식을 적용하는 것이 바람직하다.

❶ 방화벽(Firewall) 설치 운영

개인정보처리시스템으로의 접근을 IP 주소 등으로 제한하여 인가받지 않은 자를 차단하는 기능(침입차단기능)을 갖는 시스템의 설치 · 운영

- 종류 : 상태보전방식(Stateful), 상태비보존방식(Stateless)
- 형태 : 스크리닝 라우터, 단일 홈 게이트웨이, 이중 홈 게이트웨이 방식 등

❷ 침입탐지시스템(IDS : Intrusion Detection System)

개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능(침입탐지기능)을 갖는 시스템의 설치 · 운영

❸ 침입차단시스템(IPS : Intrusion Prevention System)

침입차단기능과 침입탐지기능을 결합한 침입 방지시스템을 설치 · 운영

❹ ACL(Access Control List)

라우터등 네트워크 장비에 포함되어 있는 ACL(Access Control List) 기능을 사용

- ACL에는 Standard Access List와 Extended Access List가 존재
  - Standard Access List : Source address만 참조해서 filtering 여부를 결정
  - Extended Access List : Source address 외에도 Destination address, Port, Protocol 등 다양한 정보를 참조해서 filtering 여부를 결정

※ ACL에 관한 설정은 벤더사별로 확인

특히 개발단계에서는 접속기록의 위조 · 변조 방지를 위한 조치와 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술을 적용하는 방안과 그 밖에 필요한 보호조치가 반드시 처리되어야 한다. 이에 대한 상세 내용은 본 가이드라인의 제3장 개인정보처리시스템 개발 · 구축 단계를 참조한다.

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 내부관리계획 수립 · 시행 위반 사례
  - 개인정보의 안전한 처리를 위한 내부관리계획 미수립
- 접근통제 및 접근권한의 제한 조치 위반사례
  - 개인정보취급자의 권한 부여, 변경 또는 말소내역 미기록
  - 접근권한의 보관 및 관리 위반
  - 외부에서 관리자페이지에 접속 시 VPN이나 전용선 등 안전한 접속 수단 미제공
  - 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관
  - 홈페이지 회원관리의 관리자 계정을 2명이 공유하여 사용
  - 내부관리계획으로 수립한 비밀번호 작성규칙 미수립 또는 적용 미흡
- 개인정보 저장 및 전송 시 암호화 위반사례
  - 홈페이지에서 비밀번호 저장 시 암호화 미조치
  - 홈페이지에서 비밀번호 저장 시 일방향이 아닌 양방향 암호화 조치
  - 비밀번호 및 주민등록번호 저장 시 암호화 미조치
  - 홈페이지에서 비밀번호 및 주민번호 전송 시 암호화 미조치
  - 안전하지 않은 암호 알고리즘으로 암호화 조치
- 접속기록 보관 및 위 · 변조 방지 조치 위반사례
  - 개인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력 · 열람 · 수정 등 수행업무) 관리 미흡
  - 접속기록을 6개월 이상이 아닌 3개월만 보관
- 보안프로그램 설치 및 갱신 미실시
  - 보안프로그램 업데이트 주기를 일 1회가 아닌 주 1회로 갱신
- 보관시설 마련 및 잠금장치 설치 등 물리적 조치 위반사례
  - 잠금장치가 없는 장소에 개인정보가 포함된 서류 무단 방치

6. 개인정보 저장 및 전송 시 암호화 방식 결정

개인정보를 개인정보처리시스템에 저장하거나 네트워크를 통해 전송할 때 개인정보의 불법적인 노출 또는 위 · 변조 방지를 위해 암호화를 하여야 하며, 이에 따라 기획단계에서 적절한 암호화 방식을 결정하여야 한다.

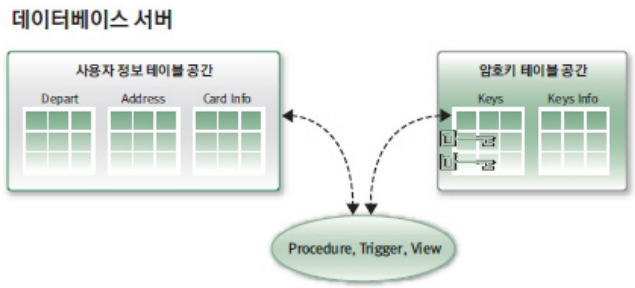
관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

암호화는 암호화 방식과 암호화 위치에 따라 다양하게 적용할 수 있으며, 대표적으로 DB 암호화, 디스크 암호화, 파일시스템 암호화에는 아래와 같은 방식으로 적용할 수 있다.

❶ DB 서버 내부에서의 암호화 구축

DB 서버가 제공하는 암호화 기능을 사용하는 경우 손쉽게 암복호화가 구현이 가능하고 DB 서버와 연계되는 애플리케이션들의 수정이 별도로 필요로 하지 않는 투명성 (Transparent)를 제공한다.
DB 암호화의 또 다른 방식은 DBMS가 제공하는 암호화 기능이 아닌 3rd Party 벤더 (Vendor)사에서 제공하는 에이전트 방식(Agent)으로 정의되는 플러그인(Plug-In)방식이다. 이 경우는 DB 서버의 부하를 발생시키지만 암호키 관리를 외부에서 수행하기 때문에 보안 취약점을 극복할 수 있는 장점이 있다.



(출처 : http://www.dbguide.net)

[그림 9] 데이터베이스 서버 내부에서의 암호화

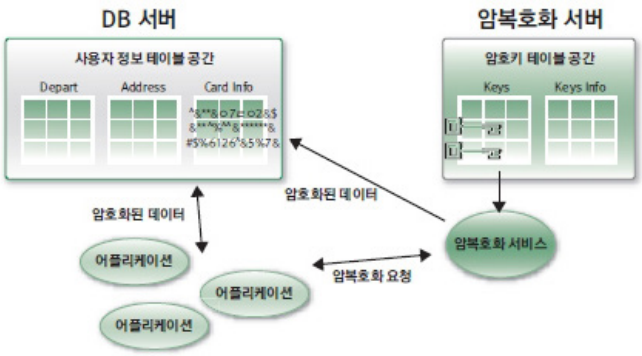
[표 4] 데이터베이스 서버 내부에서의 암호화 구축 시 장단점 비교

장점	단점
애플리케이션의 수정이 불필요	암복호화에 의한 서버 부하 발생
DBMS의 자체 암호화 기능으로 구축이 용이	DB 외부에서의 데이터 보호가 어려움
	DB 테이블내 암호키가 존재하여 보안성이 약함 별도의 암호키 분리를 위해 HSM 장비가 필요
	제한적인 암호화 알고리즘만이 지원됨

(출처 : http://www.dbguide.net)

❷ DB 서버 외부에서의 암호화 구축

DB 서버 외부에서 암호화를 구축하는 것은 애플리케이션에서 처리된 데이터는 암호화된 상태로 DB로 전송되고 안전하게 DB 내에 저장 관리되며, 반대로 요청에 의해 암호화된 데이터를 가져와서 처리하게 되는 방식이다.



(출처 : http://www.dbguide.net)

[그림 9] 데이터베이스 서버 외부에서의 암호화

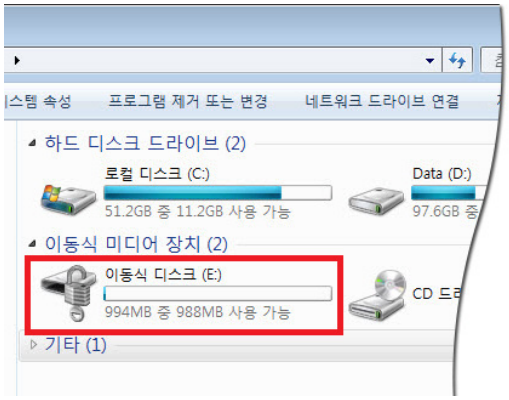
[표 5] 데이터베이스 서버 외부에서의 암호화 구축 시 장단점 비교

장점	단점
• DB 서버에서의 독립된 암호화 가능 • 암호문과 암호키의 분리로서 보안성 강화 • 암복호화 서버의 강력한 접근제어 정책으로 보안성 강화 • DB 관리자에 대한 권한분리 가능과 데이터 열람의 제한 가능 • 다수의 DB와 다수의 애플리케이션 서버의 연계 지원 가능 • DB 서버와 클라이언트의 데이터 전송시의 암호화로 유출 가능성 감소	• 통신 증가에 따른 네트워크 부하 증가 • 애플리케이션의 수정에 따른 부담 • 암복호화 서버의 부가적인 접근제어 시스템 마련 필요

(출처 : http://www.dbguide.net)

❸ 디스크 암호화

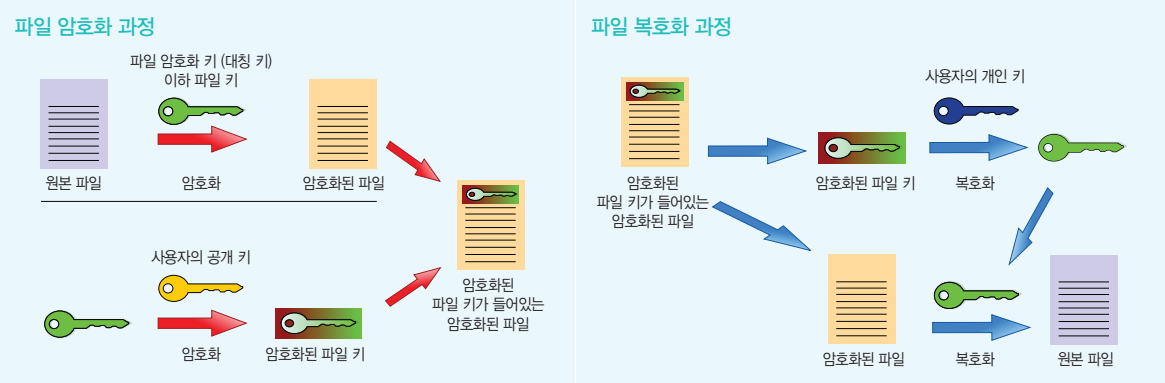
디스크를 암호화하는 도구에는 대표적으로 마이크로소프트에서 제공하는 비트로커 드라이브 암호화(BitLocker Drive Encryption)가 있다.(윈도 비스타, 윈도 서버 2008, 윈도 7, 윈도 8 운영체제에 포함된 기능)



[그림 11] 디스크 암호화 적용

❹ 파일시스템 암호화

파일시스템 암호화(EFS: Encrypting File System) 방식은 마이크로소프트 윈도의 NTFS 버전 3.0에서 추가된 파일 시스템 단계 암호화를 하는 기능이다.



[그림 12] 파일 암복호화 과정

전송구간 암호화 방식에는 SSL/TLS 또는 VPN 등을 이용하여 개인정보를 비롯한 주요 정보 등을 안전하게 송수신 할 수 있다.

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 개인정보 저장 및 전송 시 암호화 위반
  - 홈페이지에서 비밀번호 저장 시 암호화 미조치
  - 홈페이지에서 비밀번호 저장 시 일방향이 아닌 양방향 암호화 조치
  - 비밀번호 및 주민등록번호 저장 시 암호화 미조치
  - 홈페이지에서 비밀번호 및 주민번호 전송 시 암호화 미조치
  - 안전하지 않은 암호 알고리즘으로 암호화 조치

7. 개인정보 처리(취급)방침 수립

개인정보처리자는 사업 목적 및 범위 등을 고려하여 개인정보 처리방침을 수립하고 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 한다.

관련근거

① 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
② 정보통신망법 제27조2(개인정보 취급방침의 공개)

개인정보 처리방침은 '개인정보 처리방침'으로 표기하여 홈페이지의 첫 화면에 글자크기, 색깔 등을 달리하여 아래 그림과 같이 누구나 쉽게 알아볼 수 있도록 게시해야 한다. (단, 정보통신망법 적용대상인 경우에는 '개인정보 취급방침'으로 표기)

[그림 13] 개인정보처리방침 공개에 대한 예시

Tip

『개인정보보호 종합지원 포털-사업자-개인정보도우미-개인정보처리방침 만들기』를 통해 간편하게 개인정보처리방침을 작성할 수 있음

개인정보처리자가 개인정보 처리방침을 수립 시에는 아래 사항을 반드시 포함하여 수립하여야 한다.

주의사항

① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다.)
④ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다.)
⑤ 정보주체의 권리 · 의무 및 그 행사방법에 관한 사항
⑥ 처리하는 개인정보의 항목
⑦ 개인정보의 파기에 관한 사항
⑧ 개인정보 보호책임자에 관한 사항
⑨ 개인정보 처리방침의 변경에 관한 사항
⑩ 개인정보의 안전성 확보 조치에 관한 사항

단, 정보통신망법 적용대상인 정보통신서비스제공자인 경우에는 아래 사항을 포함한 개인정보 취급방침을 수립하여야 한다.

주의사항

① 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목 및 수집방법
② 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
③ 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법
④ 개인정보 취급위탁을 하는 업무의 내용 및 수탁자
⑤ 이용자 및 법정대리인의 권리와 그 행사방법
⑥ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항
⑦ 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

행정처분 사례

- 개인정보 처리방침 수립 및 공개 시 필수항목* 누락

제30조제1~2항 위반 : 1천만원 이하의 과태료(1회 200만원)

- 처리방침 수립 시 필수항목 일부 누락(위탁, 파기, 안전조치)
- 처리방침은 수립하였으나, 홈페이지 등에 미공개
- 처리방침 공개 시 필수항목 일부 누락(제3자 제공)

8. 개인정보 영향평가 고려사항

공공기관이 개인정보처리시스템을 구축 · 운용 또는 변경하려는 경우 개인정보에 대한 위험요인 분석과 개선 사항 도출을 위한 영향평가를 행정자치부장관이 지정하는 기관 중에서 의뢰하여 수행하고 그 결과를 행정자치부장관에게 제출하여야 한다.

관련근거

① 개인정보 보호법 제33조(개인정보 영향평가)

공공기관에서 아래와 같은 개인정보처리시스템을 구축 · 운영 또는 변경하려는 경우에는 반드시 개인정보 영향평가를 고려하여야 한다.

주의사항

① 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보를 처리하는 경우
② 내부 또는 외부에 있는 다른 개인정보시스템(파일)과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 경우
③ 100만명 이상의 정보주체에 관한 개인정보를 다루는 경우
④ 개인정보 영향평가를 받은 후 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우(이 경우에는 변경되는 부분으로 한정)

개인정보 영향평가는 아래와 같이 분석 · 설계 단계에서 이루어지는 것이 일반적이다.

[그림 14] 시스템 개발 단계

개인정보 영향평가를 위해 반드시 사전에 준비해 두어야 할 사항은 아래와 같다.

주의사항

① 개인정보보호를 위한 내부관리계획
② 개인정보 처리방침
③ 개인정보 흐름표
④ 개인정보 흐름도

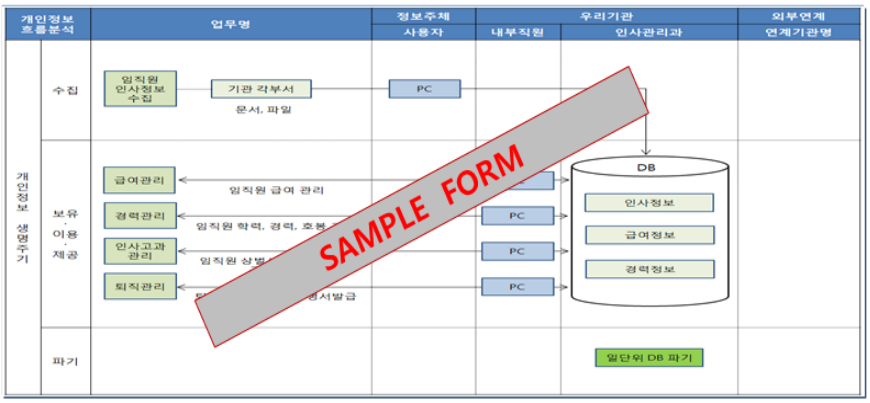
업무명	수집			보유 · 이용		
	수집항목	수집경로	수집 담당자	보유 형태	이용목적	개인정보 취급자
인사정보 수집	성명, 주민등록번호, 전화번호, 주소, 학력사항, 경력사항, 가족사항	각 부서의 파일 및 문서 형태의 개인정보	인사관리 담당자	DB	임직원의 인사정보 관리	주임기획, 팀장
급여관리				DB	임직원의 인사정보 관리	주임기획, 팀장
경력관리					임직원의 인사정보 관리	주임기획, 팀장
인사고과관리				DB	임직원의 인사정보 관리	주임기획, 팀장
퇴직관리				DB	임직원의 인사정보 관리	주임기획, 팀장

SAMPLE FORM

<제공 · 파기 흐름표>

업무명	제공				파기	
	제	제공정보	제공방법	제공목적	보관기간	파기 절차
인사정보 수집					이용목적 달성 후 지체 없이 파기	
급여관리						
인사고과관리						
퇴직관리						

[그림 15] 개인정보 흐름표 예시



[그림 16] 개인정보 흐름도 예시

9. 시큐어 코딩을 적용한 개발 방안 마련

소스코드상의 취약점은 해킹 등을 통한 개인정보 유·노출 사고의 원인이 될 수 있기 때문에 이를 예방하고자 개발 단계에서부터 보안약점을 제거하는 노력이 필요하다.

관련근거

① 전자정부법 제45조(2014.11.21.)
행정기관 및 공공기관 정보시스템 구축·운영 지침(행정자치부고시 제2014-1호)

행정기관 및 공공기관의 정보시스템 감리대상 정보화사업을 대상으로 'SW 개발보안' 의무제가 2012년 12월부터 시행되었다. 2015년 1월부터는 감리대상 전체 사업으로 확대하여 적용된다.
2014년도 SW 보안약점 기준은 아래와 같은 SQL 삽입 등 47개 항목이 대상이다.

[표 6] 소프트웨어 보안약점 항목

유형	주요내용	개수
입력 데이터 검증 및 표현	프로그램 입력 값에 대한 부적절한 검증 등으로 인해 발생할 수 있는 보안약점 예) SQL 삽입, 자원 삽입, 크로스사이트스크립트 등	15개
보안기능	인증, 접근제어, 권한 관리 등을 적절하지 않게 구현시 발생할 수 있는 보안약점 예) 부적절한 인가, 중요정보 평문저장, 하드코드된 패스워드 등	16개
시간 및 상태	멀티프로세스 동작환경에서 부적절한 시간, 상태관리로 발생할 수 있는 보안약점 예) 경쟁조건, 제어문을 사용하지 않는 재귀함수 등	2개
에러처리	불충분한 에러처리로 중요정보가 에러정보에 포함되어 발생할 수 있는 보안약점 예) 오류상황 대응 부재, 오류메시지를 통한 정보노출 등	3개
코드오류	개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점 예) 널 포인터 역참조, 부적절한 자원 해제 등	4개
캡슐화	불충분한 캡슐화로 인가되지 않은 사용자에 데이터가 노출될 수 있는 보안약점 예) 제거되지 않고 남은 디버그 코드, 시스템 데이터 정보노출 등	5개
API 오용	부적절하거나, 보안에 취약한 API 사용으로 발생할 수 있는 보안약점 예) DNS lookup에 의존한 보안결정 등	2개

시큐어코딩과 관련하여 보다 자세한 사항은 『KISA - 자료실 - 안내서/해설서』에서 '소프트웨어 개발 보안 가이드', '시큐어코딩가이드', '소프트웨어 보안약점 진단가이드' 등을 참고한다.

제5절 참조문서

- 개인정보 보호법
- 정보통신망법
- 개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)
- 표준 개인정보 보호지침(행정안전부고시 제2011-45호)
- 개인정보 영향평가에 관한 고시(행정안전부고시 제2012-59호)
- 개인정보의 기술적 · 관리적 보호조치 기준(방송통신위원회고시 제2012-50호)
- 소프트웨어 개발 보안 가이드(행정자치부, 2013.11)
- JAVA 시큐어코딩 가이드(행정자치부, 2012.9)
- C 시큐어코딩 가이드(행정자치부, 2012.9)
- Android-JAVA 시큐어코딩 가이드(행정자치부, 2011.9)
- 소프트웨어 보안약점 진단가이드(행정자치부, 2012.5)
- 홈페이지 개발보안 안내서(방송통신위원회, 2010.1)
- 개인정보보호 종합지원 포털(http://www.privacy.go.kr)
- 한국인터넷진흥원(http://www.kisa.or.kr)
- 개인정보보호 포털(https://www.i-privacy.kr)

Ⅲ. 개인정보처리시스템 개발 · 구축 단계

제1절 **목적 및 개요**

제2절 **적용범위**

제3절 **기본원칙**

제4절 **준수사항**

1. 개인정보 수집 시 동의 획득 방안 반영
2. 개인정보 파기 방안 반영
3. 안전한 비밀번호 사용을 위한 정책 반영
4. 개인(회원)정보 파일 다운로드 제한
5. 개인정보처리시스템에 대한 접근통제
6. 개인정보 저장 및 전송 시 암호화 적용
7. 접속기록, 권한변경에 대한 로깅 및 저장 관리
8. 개인정보 처리(취급)방침 공개
9. 개인정보가 포함된 출력물에 대한 보안 조치

제5절 **참고문서**

Ⅲ 개인정보처리시스템 개발 · 구축 단계

제1절 목적 및 개요

- 본 장에서는 개인정보처리시스템 개발 · 구축 단계에서 개발자들이 알아야 하는 개인정보 보호를 위한 필요한 조치사항을 기술하였다.

제2절 적용범위

- 개인정보처리시스템을 개발 · 구축(설계 및 구현)하는 단계에서 개발자들이 확인하고 적용해야 할 사항을 안내한다.

제3절 기본원칙

개인정보처리시스템을 개발 · 구축하는 단계에서 개인정보보호를 위해 검토하고 확인하여야 할 기본원칙은 아래와 같다.

- 개인정보 수집 시 관련 규정에 의한 방법으로 동의를 획득하도록 개발
- 개인정보처리 목적 달성 시 별도보관 및 완전 파기 방법 반영하여 개발
- 관리자, 사용자 및 이용자에 대한 안전한 패스워드 사용 정책을 반영
- 개인(회원)정보를 파일로 다운로드하는 기능은 제한적으로 개발
- 관리자 페이지 등에 대한 접근통제 및 권한부여 기능을 개발 시 반영
- 개인정보 전송 및 저장 시 안전한 알고리즘으로 암호화되도록 개발에 반영
- 접속기록, 권한변경에 대한 로그를 남기고 별도로 저장 관리하도록 개발
- 수립된 개인정보 처리방침을 적절한 방법으로 공개하도록 개발
- 개인정보 출력 시 마스킹(*) 처리 등 출력물에 대한 보안을 고려하여 개발

제4절 준수사항

1. 개인정보 수집 시 동의 획득 방안 반영

개인정보 수집 동의는 이용자가 개인정보를 입력하기 전 단계에 동의 사항을 공지하고 동의 여부를 선택할 수 있도록 구현해야 한다.

관련근거

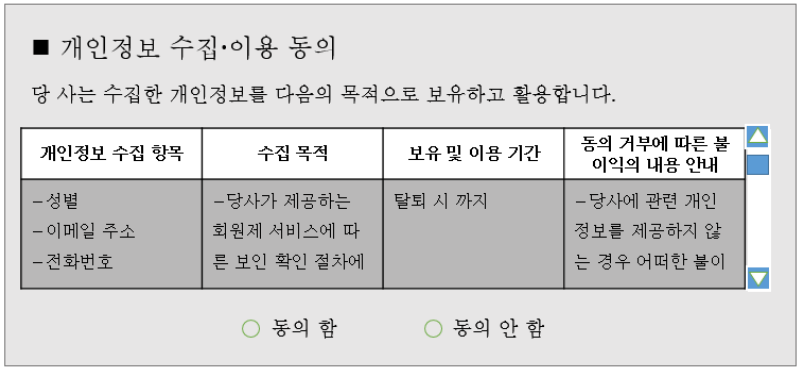
① 개인정보 보호법 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법)
② 정보통신망법 제26조의2(동의를 받는 방법)

정보 수집 동의를 얻으려면 ① 개인정보 수집 · 이용 목적, ② 수집하는 개인정보의 항목, ③ 개인정보의 보유 · 이용 기간, ④ 동의 거부시 불이익 을 모두 이용자에게 알리고 동의를 받아야 하며, 이때 이용자가 이를 명확히 이해할 수 있도록 쉽게 설명해야 한다.

① 개인정보의 수집 · 이용목적 : 예) 본인 확인, 고지 사항 전달, 물품배송

② 수집하는 개인정보의 항목 : 예) 이름, 전화번호, 접속 내역

③ 개인정보의 보유 · 이용 기간 : 예) 회원탈퇴 등 서비스 목적 달성 후 즉시 파기



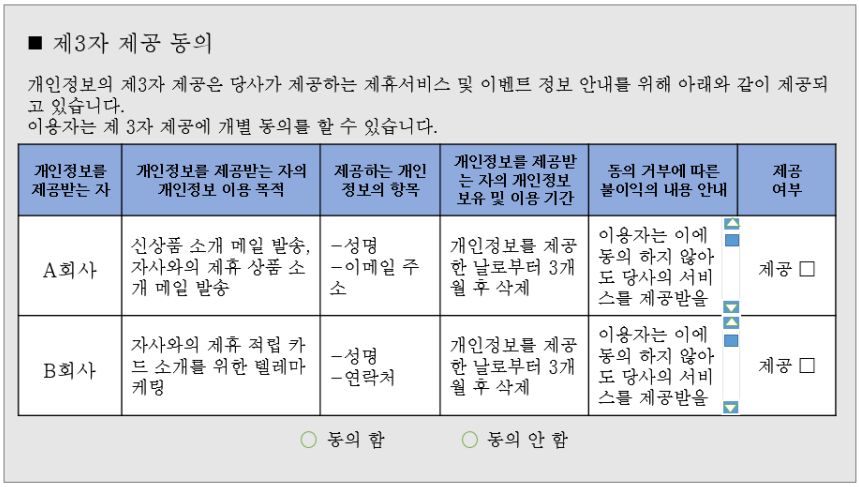
■ 개인정보 수집·이용 동의

당 사는 수집한 개인정보를 다음의 목적으로 보유하고 활용합니다.

개인정보 수집 항목	수집 목적	보유 및 이용 기간	동의 거부에 따른 불이익의 내용 안내
-성별 -이메일 주소 -전화번호	-당사가 제공하는 회원제 서비스에 따른 본인 확인 절차에	탈퇴 시 까지	-당사에 관련 개인정보를 제공하지 않는 경우 어떠한 불이

○ 동의 함 ○ 동의 안 함

[그림 17] 개인정보 수집 시 동의 받는 방법



■ 제3자 제공 동의

개인정보의 제3자 제공은 당사가 제공하는 제휴서비스 및 이벤트 정보 안내를 위해 아래와 같이 제공되고 있습니다.
이용자는 제 3자 제공에 개별 동의를 할 수 있습니다.

개인정보를 제공받는 자	개인정보를 제공받는 자의 개인정보 이용 목적	제공하는 개인정보의 항목	개인정보를 제공받는 자의 개인정보 보유 및 이용 기간	동의 거부에 따른 불이익의 내용 안내	제공 여부
A회사	신상품 소개 메일 발송, 자사와의 제휴 상품 소개 메일 발송	-성명 -이메일 주소	개인정보를 제공한 날로부터 3개월 후 삭제	이용자는 이에 동의 하지 않아도 당사의 서비스를 제공받을	제공 □
B회사	자사와의 제휴 적립 카드 소개를 위한 텔레마케팅	-성명 -연락처	개인정보를 제공한 날로부터 3개월 후 삭제	이용자는 이에 동의 하지 않아도 당사의 서비스를 제공받을	제공 □

○ 동의 함 ○ 동의 안 함

[그림 18] 개인정보 제3자 제공 동의 예시

개인정보 처리를 위탁할 때에는 개인정보 처리방침 등을 통해 위탁 관련 내용을 정보 주체에게 공개하도록 하여야 하며, 재화 · 서비스 홍보 및 판매 권유 업무를 위탁하는 경우에는 서면, 전자우편, 전화, 문자 전송 등의 방법으로 위탁 내용과 수탁자를 알리고, 알릴 수 없는 경우 홈페이지에 30일 이상 게시하여야 한다.

『정보통신망법』에 따른 정보통신서비스제공자는 개인정보 취급위탁시 별도의 동의 획득을 원칙으로 하고 있으나, '서비스 계약 내용의 이행을 위해 반드시 필요한 경우' 등의 경우에는 고지로 갈음할 수 있도록 하고 있다.

[표 7] 정보통신망법에 근거한 취급위탁 시 동의 획득에 관한 예시

구분	공개 · 통지로 처리 가능한 위탁 업무	이용자의 동의를 얻어야 하는 위탁 업무
내용	이용자와 계약을 맺은 서비스를 제공하기 위해 불가피하게 발생하는 위탁 업무	이용자와 계약한 주요 서비스 제공과는 무관한 부가적인 업무를 처리하기 위해 위탁하는 경우
예시	**(예1)** 온라인 쇼핑몰에서 물품 배송을 위해 배송업체와 계약을 맺어 배송업무를 위탁하여 처리하고 있는 경우 • 위탁하는 개인정보: 이용자의 이름, 주소 등 • 서비스 제공을 위해 불가피하게 발생하는 위탁 업무 : '물품배송업무' **(예2)** 인터넷서비스 가입계약을 맺은 경우 통신망 개통, A/S 등 서비스 제공하고 있는 경우 • 위탁하는 개인정보 : 이용자의 이름, 주소, 사용 중인 서비스 • 서비스 제공을 위해 불가피하게 발생하는 위탁 업무 : 통신망 개통, A/S 등	**(예1)** 일시적인 이벤트 혹은 경품 행사의 운영 업무를 홍보대행사에 아웃소싱 하는 경우 **(예2)** 포털 사이트 내 맞춤형 온라인 광고를 위해 포털 사이트 운영사가 온라인 광고 아웃소싱 업체에 회원 정보 제공하는 경우 **(예3)** 상기 위탁업무에 대해 이용자로부터 동의를 획득하는 업무를 위탁하는 경우

[표 8] 개인정보 수집 동의 획득 구현 시 유의 사항

구분	동의 획득 구현 시 유의 사항
이용자의 직접 동의	이용자가 동의여부를 능동적으로 결정할 수 있도록 하기 위해 미리 동의에 선택이 되어 있지 않도록 하여야 한다.
14세 미만 아동 개인정보 수집	반드시 법정대리인의 동의를 받아야 하며, 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.
별도 동의 받아야 하는 항목	기본 제공 서비스와 무관한 서비스 제공을 위해 수집이 필요한 선택 동의 항목, 민감정보, 제3자 제공, 취급위탁(정보통신망법 적용대상의 경우 검토 필요)
순차적인 동의 요구	(예시) ① [필수] 필수동의 항목에 대한 수집 · 이용 동의 → ② [선택] 선택동의 항목에 대한 수집 · 이용 동의 → ③ [선택] 취급위탁 동의 → ④ [선택] 제3자 제공 동의)
일괄동의 기능	이용자가 동의 내용을 확인한 후 개별 동의가 가능하고, 동의 여부는 강제가 아닌 선택 사항이라는 점을 명시적으로 알려야 한다. 일괄동의기능의 항목에 선택 동의 사항이 있는 경우 이 사실을 알린 후 동의를 받아야 한다.
제휴서비스 제공을 위해 '제3자 제공'이 필수적인 경우	"개인정보 수집 이용 · 동의"를 받으면서 "제3자 제공 동의"에도 함께 표시되도록 구성하는 것이 가능하다.

행정처분 사례

개인정보 수집 시 정보주체의 동의 미획득

제15조제1항 위반 : 5천만원 이하의 과태료(1회 위반 1,000만원)

- 홈페이지 상담게시판(제품관련 문의, 고객상담)에서 개인정보(성명, 연락처, 이메일) 수집 시 동의 미획득

개인정보 수집 시 필수 고지사항* 미고지

※ * 고지항목(4개) : 수집 · 이용목적, 수집항목, 보유 · 이용기간, 미동의 시 불이익 고지

제15조제2항 위반 : 3천만원 이하의 과태료(1회 위반 600만원)

- 홈페이지 통한 개인정보 수집 시 동의거부권 및 불이익 사항(1개) 고지 누락
- 홈페이지 통한 개인정보 수집 시 보유 · 이용기간(1개) 고지 누락

행정처분 사례

- 홈페이지 민원게시판에서 개인정보 수집시 필수사항 전부(4개) 고지 누락
- 홈페이지에서 고지한 수집항목과 실제 수집항목 불일치, 이용기간 불명확으로 2개 항목 고지내용 미흡
- 수집단계에서 필수/선택항목을 구분하나, 고지(안내)단계에서 필수/선택항목을 구분하지 않아 고지내용 미흡
- 지문정보 수집 시 고지내용 부정확(지문 외 불필요한 수집항목 및 수집목적 혼재, 보유기간 부정확)

동의 시 필수/선택 등 구분 동의방법 위반

제22조제1~3항 위반 : 각각 1천만원 이하의 과태료(1회 위반 200만원)

- 홈페이지에서 주민번호와 여권 정보를 일반 정보와 구분 않고 일괄 동의 받음
- 홈페이지에서 일반 정보와 마케팅 활용 정보를 구분 않고 일괄하여 동의 받음
- 제공 동의 시 수집 · 이용과 구분 동의 미실시
- 주민등록번호 수집 시 구분 동의 미실시
- 홈페이지에서 수집하는 개인정보의 목적 외 제3자 제공 동의 시 각각의 동의사항을 구분하지 않고 포괄하여 동의

선택적 사항 미동의 시 서비스 거부 금지 위반

제22조제4항 위반 : 3천만원 이하의 과태료(1회 위반 600만원)

- 홈페이지에서 선택정보인 여권번호 수집에 미동의 시 회원가입 절차가 정지 되어 서비스 이용 제한
- 마케팅 활용 목적 미동의 시 회원가입 제한

2. 개인정보 파기 방안 반영

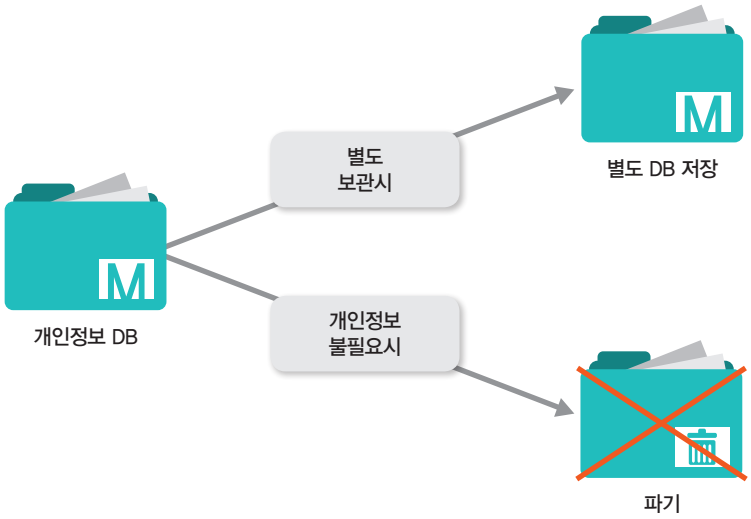
관련근거

① 개인정보 보호법 제21조(개인정보의 파기), 제29조(안전조치의무)
② 정보통신망법 제29조(개인정보의 파기)

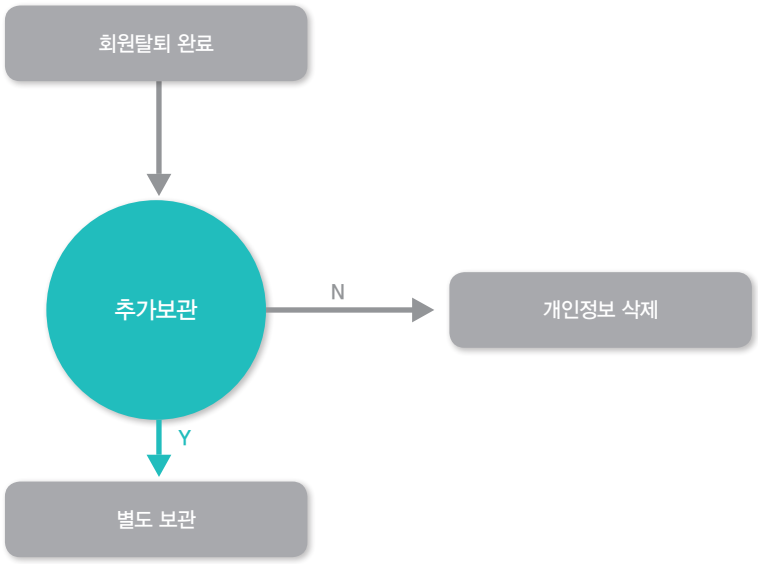
수집한 개인정보의 보유기간이 경과하거나 이용목적이 달성되어 개인정보가 더 이상 불필요하게 된 경우에는 지체 없이 개인정보를 재생 불가능한 형태로 파기해야 하며, 다른 법령상 근거에 따라 계속 보유하여야 할 필요성이 있는 경우에는 반드시 현재 이용중인 개인정보와 별도로 분리하여 보관하여야 한다.

분리 보관 방법은 별도의 DB를 생성하여 저장하거나 물리적으로 다른 서버에 저장하는 방법이 있다. 별도로 보관하는 개인정보DB의 경우 일반 개인정보DB의 접근권한 과 다르게 설정하여 불필요한 접근 · 조회 · 유출을 방지할 필요가 있다.

파기 절차를 자동화하기 위해 회원이 탈퇴를 완료한 후에 자동으로 탈퇴한 회원의 개인정보가 DB에서 삭제될 수 있도록 할 수 있으며, 법령상 근거에 따라 회원탈퇴 이후에도 추가로 보관이 필요한 경우(예를 들어, 전자상거래법에 따른 거래기록 보관 등) 별도의 DB에 저장될 수 있도록 구성할 수 있다. 그리고 회원가입 시 개인정보 보유 기간을 DB에 함께 저장해 보유기간이 경과한 개인정보는 자동 삭제되도록 하는 방식으로 불필요한 개인정보를 삭제



[그림 19] 개인정보 파기 또는 분리저장



[그림 20] 개인정보 삭제 흐름도

할 수 있다.

개인정보를 파기할 때에는 로우레벨 포맷이나 천공, 파쇄 등 재생 · 복구가 불가능한 방법으로 파기하여야 한다. 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기적으로 기록된 개인정보의 경우에는 기술적 방법으로 재생 불가능하도록 하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 해야 한다. 그리고 원본 데이터 외에 백업 데이터가 존재하는지 여부를 확인한 후 파기하여야 한다.

기록물, 인쇄물 등 파쇄가 가능한 형태인 경우에는 파쇄기 등을 이용하여 물리적으로 파쇄하거나 소각해야 한다.

[표 9] 개인정보 완전 파기 방법

파기 종류	파기 방법
프로그램을 이용한 파기	로우레벨 포맷(초기화), 와이핑(덮어쓰기)
물리적인 파기	천공, 소각, 파쇄, 디가우저(전용 소자장비)

개인정보의 일부만을 파기하는 경우 아래와 같이 조치하여야 한다. 예를 들어, 주민등록번호를 삭제하는 조치로 주민등록번호 뒤 6자리를 마스킹 처리하는 경우 필드 전체를 삭제한 후 새로 생성하는 등의 방법을 통해 쉽게 재생할 수 없는 상태로 삭제하여야 한다.

[표 10] 개인정보의 일부만을 파기하는 경우 파기 방법

구분	파기 방법
전자적 파일 형태	개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
기록물, 인쇄물, 서면, 그 밖의 기록매체	해당 부분을 마스킹, 천공 등으로 삭제

복구 및 재생할 수 없는 파기 방법(예시)

1. 하드 디스크 등 매체 전체의 데이터를 파기하는 경우

- 프로그램을 이용한 파기
  - 하드디스크, USB 메모리의 경우 '로우레벨포멧(Low level format)' 방법으로 파기
    ※ 로우레벨포멧 : 하드디스크를 공장에서 나온 초기상태로 만들어주는 포맷
  - 0, 1 혹은 랜덤 값으로 기존 데이터를 여러 번 덮어씌우는 와이핑(Wiping) 방법으로 파기
- 물리적인 파기
  - 데이터가 저장되는 디스크 플레터에 강력한 힘으로 구멍을 내어 복구가 불가능하도록 하는 천공 방법으로 파기
  - CD/DVD의 경우 가위 등으로 작은 입자로 조각내거나, 전용 CD파쇄기나 CD파쇄가 가능한 문서파쇄기 등을 이용하여 파기
  - 고온에 불타는 종류의 매체는 소각하는 방법으로 파기
  - 자기장치를 이용해 강한 자기장으로 데이터를 복구 불가능하게 하는 디가우저(Degausser) 파기

2. 고객 서비스에 이용 중인 DB서버에 저장된 일부 데이터를 파기하는 경우

- 서비스 중인 DB의 해당 개인정보 위에 임의의 값(Null값 등)을 덮어쓰기 한 후 삭제(delete)
- DB의 특정부부에 덮어쓰기가 곤란한 경우에는 테이블 데이터에 대한 논리적인 삭제(delete)도 허용되나, 신속하게 다른 데이터로 덮어쓰기(overwriting) 될 수 있도록 운영

행정처분 위반

- 보유기간 경과, 처리목적 달성 후 개인정보 미파기

제21조제1항 위반 : 3천만원 이하의 과태료(1회 위반 600만원)

- 홈페이지에서 탈퇴한 회원정보 일부 또는 전부 미파기
- 보유기간을 경과하거나 수집목적을 달성한 개인정보 미파기
- 보존기간이 경과된 개인정보(이름/연락처/성별) 미파기

3. 안전한 비밀번호 사용을 위한 정책 반영

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

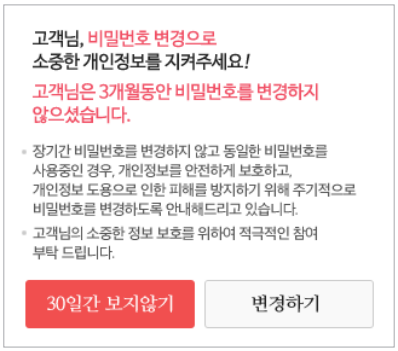
개발자는 비밀번호 정책을 수립하여 개발시에 이를 반영하여야 한다. 비밀번호 정책은 아래와 같은 사항을 기본적으로 반영해야 하며, 개발 요구사항에 별도로 비밀번호와 관련된 정책이 명시되어 있다면 개발 요구사항에 포함된 내용까지도 함께 고려해야 한다. 이 때 요구사항 정책이 아래 내용과 다를 경우 보다 높은 강도의 정책을 반영하도록 한다.

[표 11] 개발 시 비밀번호 적용 규칙

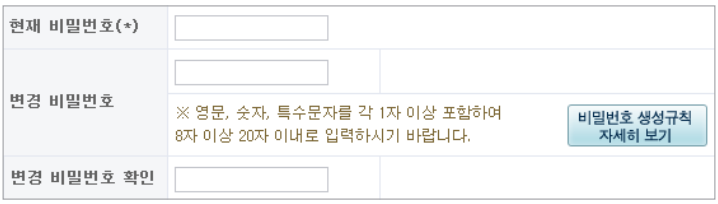
구분	개발 시 비밀번호 적용 규칙
비밀번호의 최소 길이	비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하도록 개발하여야 함 • 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우 • 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우 ※ 컴퓨터 관련 기술의 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있고, 변경주기는 짧아질 수 있다.
추측하기 어려운 비밀번호의 생성	• 생성하는 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 못하도록 개발하여야 함 • love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 못하도록 개발하여야 함
비밀번호의 주기적인 변경	• 비밀번호에 유효기간을 설정(최소 6개월)하여 유효기간이 경과 시에는 비밀번호 변경을 요구하도록 알려주는 기능을 개발하여야 함
동일한 비밀번호 사용 제한	• 비밀번호 변경시 이전 비밀번호를 교대로 사용하지 못하도록 이전 비밀번호를 일정 개수 이상 사용하지 못하도록 개발하여야 함

※ 「KISA 암호이용활성화(http://seed.kisa.or.kr) – 국산암호보급 – 패스워드 안전성 검증」통해 비밀번호에 대한 안전성 검증 가능

비밀번호는 주기적으로 변경을 유도할 수 있도록 해야 하며 개인정보 유출 사고 등이 발생할 경우 비밀번호를 변경할 수 있도록 안내해야 한다. 비밀번호 변경 기능을 구현할 경우에는 아래 그림과 같이 현재 비밀번호를 확인하는 필드를 두어야 하며, 변경하려는 비밀번호가 현재 비밀번호와 같은 경우에는 변경되지 않도록 조치한다.



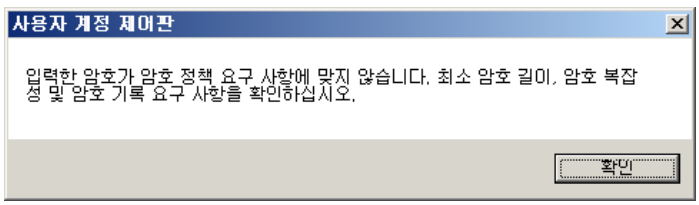
[그림 21] 비밀번호 변경주기 경과 안내 예시 화면



[그림 22] 비밀번호 변경 화면 예시

입력한 비밀번호가 비밀번호 정책에 맞지 않을 경우 아래와 그림과 같이 해당 사항에 부합된 내용을 포함한 경고창을 띄어주도록 개발한다.

[그림 23] 비밀번호가 정책에 맞지 않을 경우 화면 예시



[그림 24] 비밀번호 정책이 맞지 않는 경우 경고창 예시

행정처분 위반

- 접근통제 및 접근권한의 제한 조치 위반

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 내부관리계획으로 수립한 비밀번호 작성규칙 미수립 또는 적용 미흡

4. 개인(회원)정보 파일 다운로드 제한

개인정보처리자는 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 적절한 보안조치를 취하여야 한다.

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

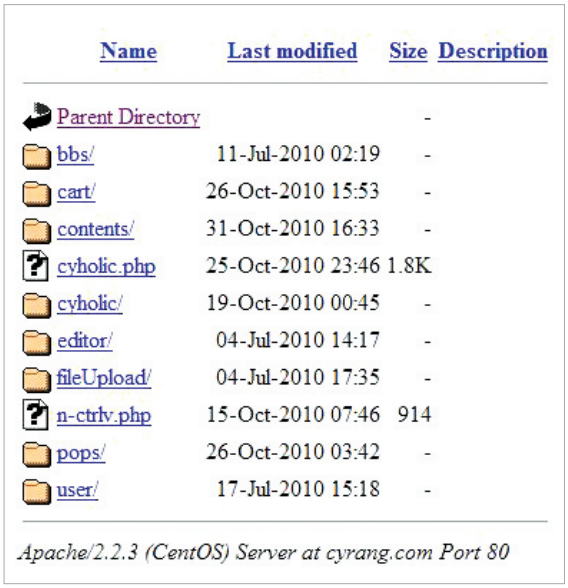
과실로 인한 인터넷 홈페이지에서 노출 방지

웹사이트를 통해 고객의 개인정보를 수집 · 관리하는 경우에는 ID 및 비밀번호를 통한 사용자 인증(Login) 기능을 적용하여야 한다. 또한, 수시로 웹 사이트 게시판 등에서의 주민번호 노출 여부 등을 점검하여 조치하여야 한다.

검색엔진을 통한 개인정보 노출 제한

웹사이트 개발 · 구축 시 보안기준을 따르지 않아 발생하는 취약점으로 인해 구글 등의 검색 엔진을 통해 개인정보 DB가 노출될 수 있다. 그러므로 수시로 웹사이트의 취약점을 점검하여 조치하도록 한다.

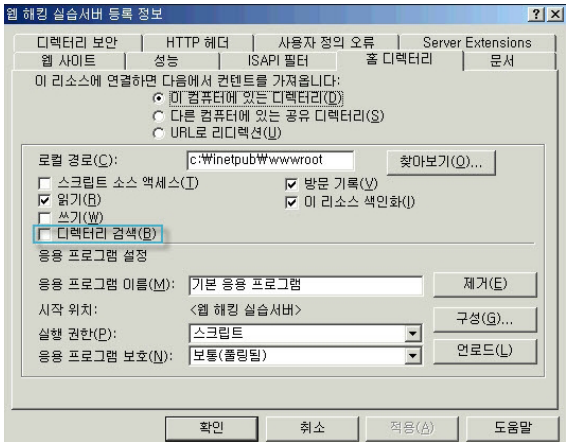
[그림 25] 검색 엔진에 노출된 개인정보 예시



Name	Last modified	Size	Description
Parent Directory		-	
bbs/	11-Jul-2010 02:19	-	
cart/	26-Oct-2010 15:53	-	
contents/	31-Oct-2010 16:33	-	
cyholic.php	25-Oct-2010 23:46	1.8K	
cyholic/	19-Oct-2010 00:45	-	
editor/	04-Jul-2010 14:17	-	
fileUpload/	04-Jul-2010 17:35	-	
n-ctrlv.php	15-Oct-2010 07:46	914	
pops/	26-Oct-2010 03:42	-	
user/	17-Jul-2010 15:18	-	

Apache/2.2.3 (CentOS) Server at cyrang.com Port 80

[그림 26] 디렉토리 리스팅



[그림 27] IIS 디렉토리 리스팅 조치방안

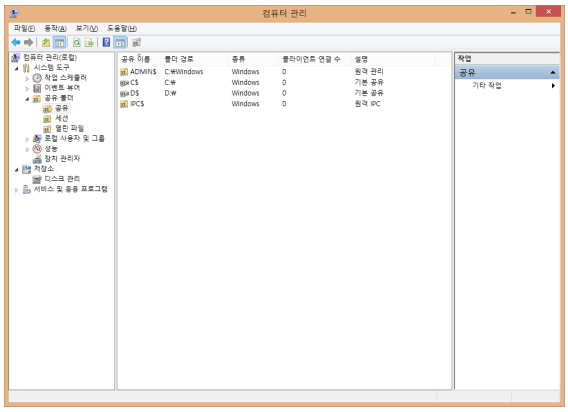
```
# vi httpd.conf
<Directory "/usr/local/apache2/htdocs">
    Options ~~Indexes~~ FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

Options에 Indexes 삭제!!
```

[그림 28] 아파치 디렉토리 리스팅 조치방안

※ 『KISA-자료실 – 관련법령 – 안내서 · 해설서-웹서버구축 보안점검 안내』 참조

공유설정을 통한 개인정보 노출 방지

공유설정 부주의로 개인정보파일이 권한이 없는 자에게 노출 될 수 있다. 따라서 공유폴더를 사용할 경우 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.



※ 윈도우즈의 경우 시작–제어판–성능 및 유지관리–관리도구–컴퓨터관리를 실행하여 공유폴더 메뉴에서 확인 가능

[그림 29] 공유폴더 설정

행정처분 사례

접근통제 및 접근권한의 제한 조치 위반

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 개인정보취급자의 권한 부여, 변경 또는 말소내역 미기록
- 접근권한의 보관 및 관리 위반
- 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관

접속기록 보관 및 위 · 변조 방지 조치 위반

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

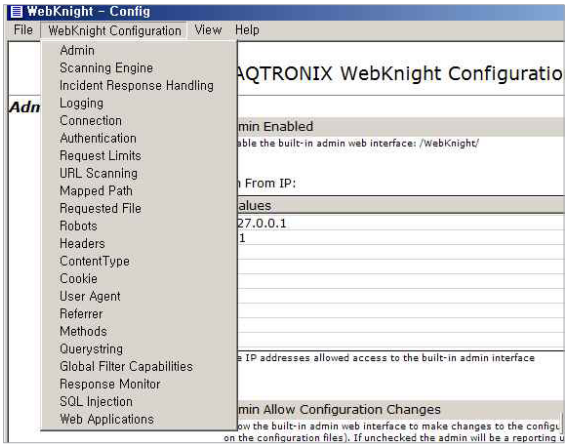
- 개인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력 · 열람 · 수정 등 수행업무) 관리 미흡
- 접속기록을 6개월 이상이 아닌 3개월만 보관

5. 개인정보처리시스템에 대한 접근통제

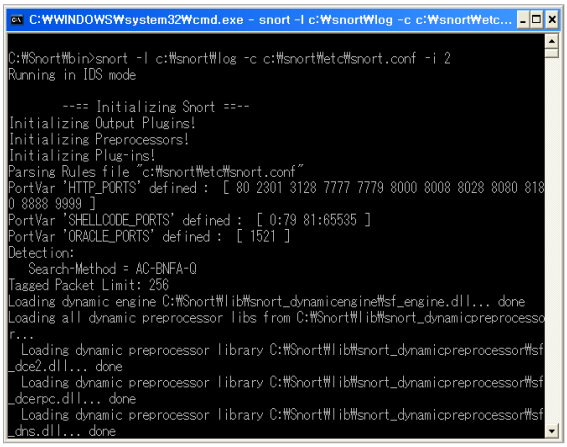
관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위해 접속 권한을 제한하여 인가받지 않은 접근을 제한하고 접속한 IP주소 등을 분석하여 불법적인 개인 정보 유출 시도를 탐지해야 한다.
접근통제 방법으로는 ACL(Access Control List), 방화벽, 무료 침입탐지시스템(Snort) 등이 있다.

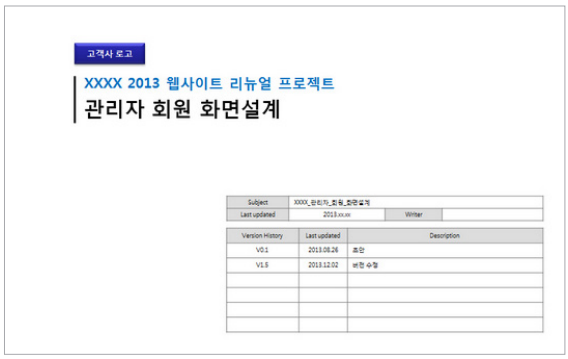


[그림 30] WebKnight 설정 화면



[그림 31] Snort 실행 화면

관리자 페이지는 http://www.test.co.kr/admin/index.php와 같이 사용자 페이지와 구분해서 별도로 개발한다.(단 admin과 같이 관리자 페이지를 유추하기 쉬운 단어는 사용하지 않는다.)



[그림 32] 관리자 화면 별도 설계

[그림 33] 관리자 모드 로그인 예시 화면

관리자 페이지가 검색엔진 등에 노출되지 않도록 로봇배제표준을 적용한다. 로봇배제표준은 웹사이트 검색로봇이 접근하는 것을 방지하기 위한 국제 규약으로, 일반적으로 접근 제한에 대한 설명을 robots.txt에 기술한다.

```
모든 로봇에게 문서접근을 "허락"하는 경우
User-agent: *
Allow: /
모든 로봇에게 문서접근을 "차단"하는 경우
User-agent: *
Disallow: /
```

※ 로봇배제표준에 관한 자세한 사항은 http://www.robotstxt.org/robotstxt.html에서 확인 가능

행정처분 사례

접근통제 및 접근권한의 제한 조치 위반

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 개인정보취급자의 권한 부여, 변경 또는 말소내역 미기록
- 접근권한의 보관 및 관리 위반
- 외부에서 관리자페이지에 접속 시 VPN이나 전용선 등 안전한 접속 수단 미제공
- 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관
- 홈페이지 회원관리의 관리자 계정을 2명이 공유하여 사용

접속기록 보관 및 위 · 변조 방지 조치 위반

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 개인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력 · 열람 · 수정 등 수행업무) 관리 미흡
- 접속기록을 6개월 이상이 아닌 3개월만 보관

6. 개인정보 저장 및 전송 시 암호화 적용

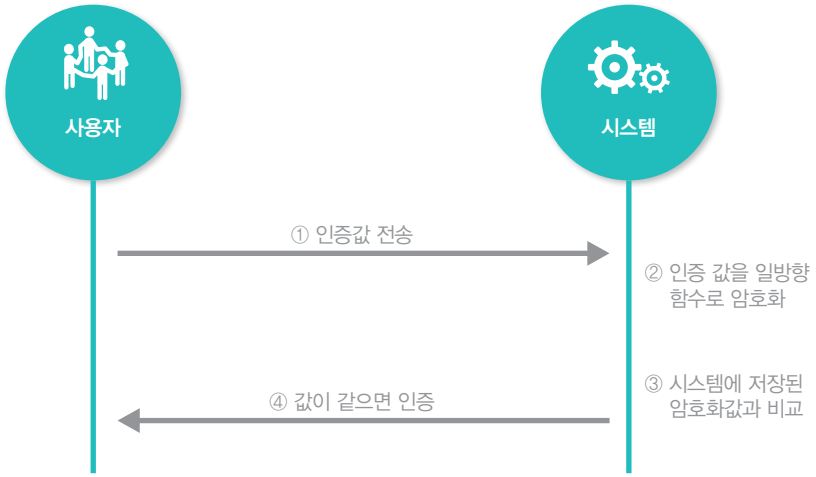
관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

개인정보를 개인정보처리시스템에 저장하거나 네트워크를 통해 전송할 때에는 불법적인 노출 또는 위 · 변조 방지를 위해 암호화를 하여야 한다.

❶ 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

비밀번호 확인 시 사용자가 입력한 비밀번호를 일방향 암호화하여 시스템에 저장된 값과 비교하는 방식으로 적용한다.



[그림 34] 비밀번호 일방향 저장 시 인증 검증 방식

❷ 비밀번호 분실 시 복호화가 불가능하므로 임의의 비밀번호 제공 또는 재설정을 할 수 있는 기능을 포함하여 개발한다.

[그림 35] 비밀번호 분실 시 비밀번호 재설정 화면 예시

❸ 일방향 암호화 적용 시에는 아래의 보안강도에 따른 해쉬 함수 분류를 참고하여 적용한다.

[표 12] 보안강도에 따른 해쉬함수 분류

보안강도	해쉬 함수	안전성
80비트 미만	MD5, SHA-1	권고하지 않음
80비트	HAS-160	
112비트	SHA-224	2013년까지 권고함
128비트	SHA-256	2013년 이후에도 가능
192비트	SHA-384	
256비트	SHA-512	

※ 출처: 개인정보의 기술적 · 관리적 보호조치 기준 해설서

```
<%@page language="java" contentType="text/html;charset=EUC-KR"
pageEncoding="EUC-KR"%>
<%@page import="sun.misc.BASE64Encoder"%>
<%@page import="java.io.*"%>
<%@page import="KISA.SHA256"%>
<%
    String sPlainText = request.getParameter( "iPlainText" );
    ☞ 웹페이지에서 메시지를 가져오는 명령어
    SHA256 s = new SHA256( sPlainText.getBytes() );
    ☞ SHA256.class에 정의된 오브젝트 생성
    BASE64Encoder Base64Encoder = new BASE64Encoder();
    ☞ Base64인코더 오브젝트 생성
    out.print( Base64Encoder.encode(s.GetHashCode()) );
    ☞ 해쉬 수행 및 웹페이지에 해쉬한 값을 출력하는 명령어
    ☞ DB 저장 : Base64Encoder.encode(s.GetHashCode())의 결과를 DB에 저장하는
          명령어로 수정
    ☞ ex) DBconn.Execute( "INSERT INTO 저장할 테이블(필드명) values
       ( '" & Base64Encoder.encode(s.GetHashCode()) & "' )" )
%>
```

[그림 36] SHA256 Hash Encode

❹ 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등 고유식별정보 및 지문, 홍채, 음성, 필적 등 바이오정보는 안전한 암호알고리즘으로 암호화하여 저장해야 한다. 이 때 아래와 같은 보안강도에 따른 대칭키 암호 알고리즘 분류를 참고하여 적용한다.

[표 13] 안강도에 따른 대칭키 암호 알고리즘 분류

보안강도	해쉬 함수	안전성
80비트 미만	DES	권고하지 않음
80비트	2TDEA	
112비트	3TDEA	
128비트	SEED, HIGHT, ARIA-128, AES-128	권고함
192비트	ARIA-192, AES-192	
256비트	ARIA-256, AES-256	

※ 3TDEA는 112비트 이상의 보안강도를 가지고 있지만, 보안성이 낮다고 평가되어 권고하지 않음
※ 출처: 개인정보의 기술적 · 관리적 보호조치 기준 해설서

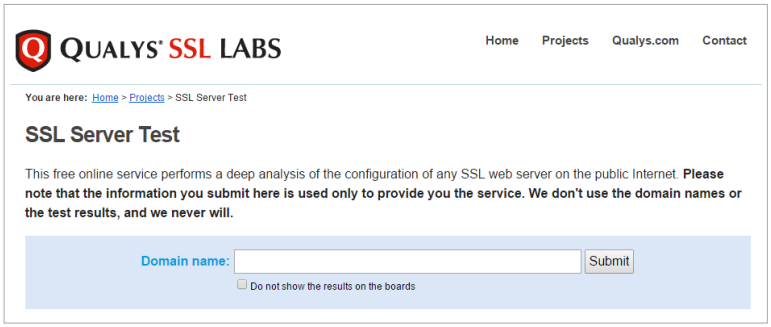
❺ 개인정보를 전송하는 전송로 구간에서는 SSL/TLS 등의 암호화 방식을 적용하여 개인정보를 보호할 수 있다.

[그림 37] SSL/TLS 암호화 적용

SSL 인증서 발급 : http://www.crosscert.com/symantec/02_0_00.jsp

SSL 취약성 여부 확인 : https://www.ssllabs.com/ssltest/

※ 세부사항은『KISA-자료실 – 관련법령 – 안내서 · 해설서 – 암호기술 구현 안내서』참조



[그림 38] SSL 취약성 여부 확인 사이트

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

개인정보 저장 및 전송 시 암호화 위반

- 홈페이지에서 비밀번호 저장 시 암호화 미조치
- 홈페이지에서 비밀번호 저장 시 일방향이 아닌 양방향 암호화 조치
- 비밀번호 및 주민등록번호 저장 시 암호화 미조치
- 홈페이지에서 비밀번호 및 주민번호 전송 시 암호화 미조치
- 안전하지 않은 암호 알고리즘으로 암호화 조치

7. 접속기록, 권한변경에 대한 로깅 및 저장 관리

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

개인정보처리자는 개인정보시스템의 접속기록을 최소 6개월 이상 보관 및 관리하여야 한다. 접속기록은 개인정보의 입 · 출력 및 수정, 파일별 · 담당자별 데이터접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 불법적인 접근을 확인할 수 있는 중요한 자료이다.

❶ 접속기록에 대해 일정기간 저장될 수 있도록 개발

개인정보취급자 등이 개인정보처리시스템에 접속하여 개인정보를 처리한 경우에는 아래 표와 같은 내용을 포함한 접속기록을 최소 6개월 이상 저장하도록 개발한다.

[표 14] 접속기록 예시

필수 기록 항목	설명
ID	개인정보취급자 식별정보
날짜 및 시간	접속일시
접속자 IP 주소	접속지 정보
수행 업무	열람, 수정, 삭제, 인쇄, 입력 등

※ 출처: 개인정보의 안전성 확보조치 기준 해설서

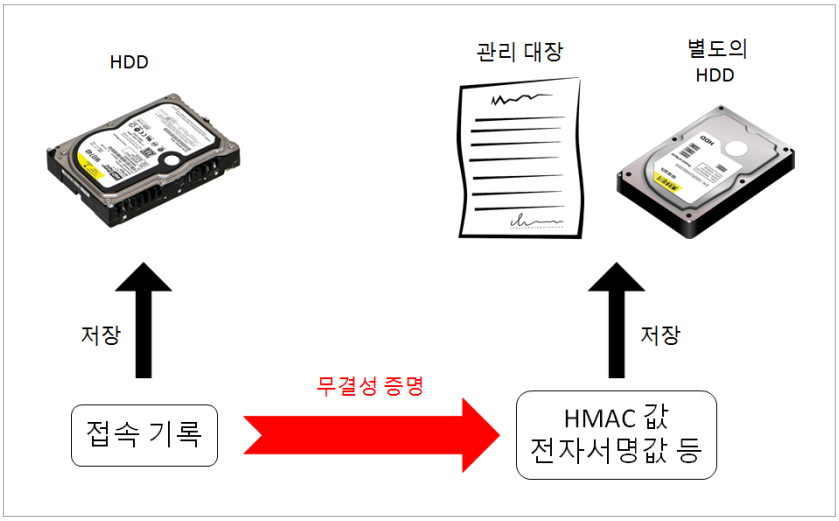
❷ 접속기록 백업

- 데이터 손실에 대비하여 별도의 물리적인 저장 장치에 보관하고 정기적인 백업 수행
- 접속기록의 위 · 변조를 방지를 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용
- 수정 가능한 매체(HDD 또는 테이프)에 접속기록을 백업하는 경우에는 무결성 보장을 위해 위 · 변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관 · 관리

  ※ 접속기록을 HDD에 보관하고, 위 · 변조 여부를 확인할 수 있는 정보(HMAC 값 또는 전자서명값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리 가능

취급자 식별정보	정보주체 식별정보	접속일시	접속지	수행업무
홍길동(K00050)	성춘향(850301)	20XX.05.01 15:00:00	172.168.11.11	온라인상담

[그림 39] 접속 기록 생성 예시



[그림 40] 접속 기록 백업 방안

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

접근통제 및 접근권한의 제한 조치 위반

- 홈개인정보취급자의 권한 부여, 변경 또는 말소내역 미기록
- 접근권한의 보관 및 관리 위반
- 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관

접속기록 보관 및 위 · 변조 방지 조치 위반

- 개인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력 · 열람 · 수정 등 수행업무) 관리 미흡
- 접속기록을 6개월 이상이 아닌 3개월만 보관

8. 개인정보 처리(취급)방침 공개

관련근거

① 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
② 정보통신망법 제27조2(개인정보 취급방침의 공개)

개인정보처리자는 개인정보 처리방침을 수립하고 정보주체가 언제든지 쉽게 확인할 수 있도록 홈페이지 등에 공개하여야 한다.

개인정보 처리방침을 홈페이지 등에 링크할 때에는 『개인정보 처리방침』으로 표기해야 하며(정보통신서비스제공자의 경우에는 정보통신망법에 의거하여 『개인정보 취급방침』으로 표기 가능), 눈에 잘 띌 수 있도록 색상, 글자크기 등을 달리하여 표시하여야 한다.

[그림 41] 개인정보처리방침 홈페이지 링크 예시

행정처분 사례

● 개인정보 처리방침 수립 및 공개 시 필수항목* 누락

※ 필수항목(8개) : 처리 목적, 처리 및 보유 기간, 제3자 제공, 위탁, 정보주체 권리 · 의무 및 행사방법, 처리 항목, 파기 사항, 안전성 확보조치

제30조제1~2항 위반 : 1천만원 이하의 과태료(1회 200만원)

- 처리방침 수립 시 필수항목 일부 누락(위탁, 파기, 안전조치)
- 처리방침은 수립하였으나, 홈페이지 등에 미공개
- 처리방침 공개 시 필수항목 일부 누락(제3자 제공)

9. 개인정보가 포함된 출력물에 대한 보안 조치

관련근거

① 정보통신망법 제28조(개인정보의 보호조치)

개인정보가 포함된 파일을 인쇄하거나 화면에 출력할 때에는 그 용도를 명확히 특정하고 용도에 따라 출력 항목을 최소화하여야 한다.

예를 들어 대리점, 고객 상담, 영업 등 업무에 대하여 각각의 업무 형태나 개인정보처리시스템의 접근권한에 따라 보여지는 출력항목을 다르게 설정한다.

[표 15] 업무에 따라 다른 출력항목 예시

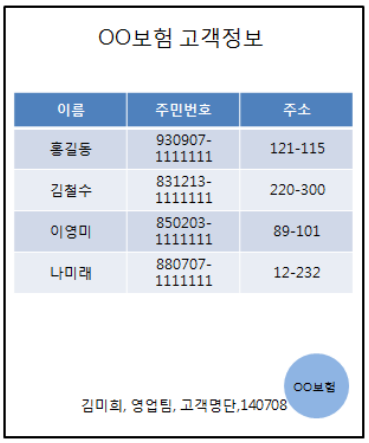
고객번호	이름	성별	주소	고객번호	등급	이름	성별	주소	전화번호
1	한지민	여	마포구	1	A	한지민	여	마포구	1234-5678
2	한효주	여	은평구	2	B	한효주	여	은평구	3456-7890
3	김고은	여	강남구	3	C	김고은	여	강남구	5678-9012

개인정보가 포함된 인쇄물, 개인정보가 저장된 보조저장매체 등 개인정보의 출력 · 복사물을 안전하게 관리하기 위하여 반 · 출입 사항을 기록하거나 별도의 로그로 남겨놓는 조치를 하여야 한다.

[표 16] 출력 · 저장 기록 예시

처리내용	처리자	처리일시	접속지
출력	홍길동	2014.12.12. 15:00:00	192.168.1.1
USB저장	김갑수	2014.12.14. 13:12:34	192.168.1.100

인쇄물 출력 시에는 필요한 경우 출력자, 부서명, 문서명, 출력일자, 회사 로고 등을 프린트 워터마킹 기술을 이용하여 삽입함으로써 출력물에 대한 보안 조치를 취하거나 DRM 등의 문서보안 솔루션을 이용해 개인정보 파일을 암호화 하는 등 적절한 보안조치를 해야 한다.



OO보험 고객정보

이름	주민번호	주소
홍길동	930907-1111111	121-115
김철수	831213-1111111	220-300
이영미	850203-1111111	89-101
나미래	880707-1111111	12-232

김미희, 영업팀, 고객명단,140708

OO보험

[그림 42] 출력물 보안 조치 예시

개인정보에 대한 마스킹(*) 처리 원칙은 다음과 같다.

주의사항

① 성명 중 이름의 첫 번째 글자 이상
② 생년월일
③ 전화번호 또는 휴대폰 전화번호의 국번
④ 주소의 읍면동
⑤ IP주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

이름 : 홍*동	휴대폰 : 010-****-1234
주민등록번호 : 19900101-1******	주소 : 서울 종로구 **동 12-3
생년월일 : ****년 *월 *일	IPv4 : 123.123.***.123
전화번호 : 02-****-1234	IPv6 : ff00:12:34:12:34:12:****:0

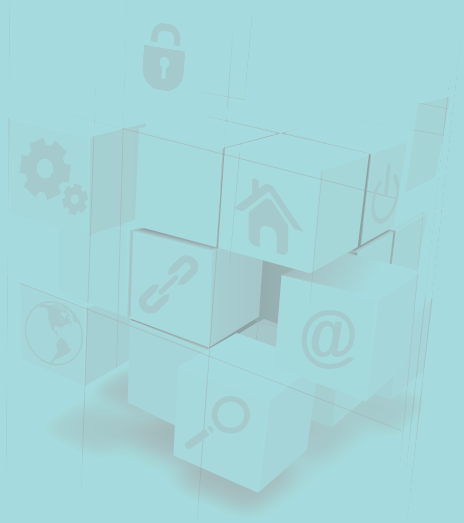
[그림 43] 개인정보 마스킹(*) 처리 화면 예시

제5절 참조문서

- 개인정보 보호법
- 정보통신망법
- 개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)
- 표준 개인정보 보호지침(행정안전부고시 제2011-45호)
- 개인정보의 기술적 · 관리적 보호조치 기준(방송통신위원회고시 제2012-50호)
- 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서
- 암호이용 안내서(방송통신위원회, 한국인터넷진흥원)
- 개인정보보호 종합지원 포털(http://www.privacy.go.kr)
- 한국인터넷진흥원(http://www.kisa.or.kr)
- 개인정보보호 포털(https://www.i-privacy.kr)

Ⅳ. 개인정보처리시스템 운영 단계

제1절 **목적 및 개요**
제2절 **적용범위**
제3절 **기본원칙**
제4절 **준수사항**
1. 개인정보처리 위탁 시 준수사항
2. 개인정보처리시스템 원격접속 시 보안 조치
3. 개인정보처리시스템 취약점 진단
4. 개인정보처리시스템 접속기록 및 접근권한 검토
5. 개인정보 유출 시 신고
6. 개인정보 이용내역 통지
제5절 **참조문서**



Ⅳ 개인정보처리시스템 운영 단계

제1절 목적 및 개요

본 장에서는 개인정보처리시스템 운영 단계에서 개발자들이 알아야 하는 개인정보 보호를 위한 필요한 조치사항을 기술하였다.

제2절 적용범위

개인정보처리시스템을 운영(운영 및 폐기)하는 단계에서 개발자들이 확인하고 적용해야 할 사항을 안내한다.

제3절 기본원칙

개인정보처리시스템을 운영하는 단계에서 개인정보보호를 위해 검토하고 확인하여야 할 기본원칙은 아래와 같다.

- 개인정보처리 업무 위탁 운영 시 적절한 관리 방안 마련 및 이행
- 관리자 페이지에 대해 원격접속 시 보안 조치 사항 반영
- 개인정보처리시스템에 대해 주기적으로 취약점 진단 수행
- 개인정보처리시스템에 대한 접속기록 및 접근권한 주기적 검토
- 개인정보 처리 과정에서 개인정보 유출 시 정보주체 통지 및 전문기관 신고
- 수집한 개인정보에 대해서는 그 이용내역의 주기적인 통지

제4절 준수사항

1. 개인정보처리 위탁 시 준수사항

관련근거

① 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
② 정보통신망법 제25조(개인정보의 취급위탁)

개인정보처리자가 업무의 효율을 위해 개인정보처리 업무를 위탁할 때에는 아래의 사항을 포함하여 문서(계약서 등)로 하고 주기적으로 이행 점검을 하도록 한다.

주의사항

① 위탁 업무의 범위와 목적에 관한 사항
② 위탁 목적 외 처리 금지에 관한 사항
③ 재위탁 제한에 관한 사항
④ 위탁하는 개인정보의 안전성 확보 조치에 관한 사항
⑤ 개인정보 관리 현황 점검 등 관리감독에 관한 사항
⑥ 수탁자의 손해배상 등 책임에 관한 사항

개인정보처리자는 개인정보 처리업무 위탁에 관한 사항을 홈페이지 등에 정보주체가 알기 쉽도록 공개하여야 한다. 개인정보처리방침에 이를 포함하여 공개하는 것도 가능하다.

행정처분 사례

- 위탁 시 필수사항*을 문서(계약서)에 미반영

  제26조제1항 위반 : 3천만원 이하의 과태로(1회 위반 600만원)

  - 위탁 시 필수사항을 문서에 일부 또는 전부 누락

- 개인정보처리 수탁사 미공개

  제26조제2항 위반 : 1천만원 이하의 과태로(1회 위반 200만원)

  - 수탁자를 홈페이지에 공개하지 않음
  - 수탁자 00개소 중 0개소 공개 누락

- 개인정보처리 수탁사 미공개

  제26조제4항 위반 : 시정조치 명령

  - 개인정보보호 수탁사 교육 및 실태점검 등 관리?감독 미실시

2. 개인정보처리시스템 원격접속 시 보안 조치

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

인가되지 않은 자의 네트워크를 통한 불법적인 접근 또는 공격 행위를 방지하기 위해 방화벽이나 IDS/PS와 같은 IP, Port 기반 차단 솔루션을 구축하거나 Secure OS 또는 OS 자체의 접근제어를 통해 불법적인 접근에 대한 보안 조치를 해야 한다. 또, 원격으로 접속하는 경우 VPN(penvpn, ipsec 등) 또는 전용선과 같은 안전한 접속 수단을 구축해야 한다. (https 방식은 권장하지 않음)

[표 17] H/W, S/W 보안 조치 분류

구분	조치 방안
불법적인 침입 차단 조치	FW, IDS, IPS, UTM 등 Secure OS, 자체 접근제어 등
안전한 접속을 위한 조치	VPN, 전용선, 공인인증서 등

만일 개인정보처리자가 개인정보처리시스템 대신 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우 운영체제 등에서 제공하는 접근통제 기능을 사용할 수 있다.

[표 18] 개인정보처리시스템 사용 여부에 따른 접근통제 방법

구분	차단, 탐지 시스템	VPN 구축	자체 접근통제 기능
개인정보처리시스템 사용	○	○	×
업무용 컴퓨터만 사용	×	○	○

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 접근통제 및 접근권한의 제한 조치 위반
  - 외부에서 관리자페이지에 접속 시 VPN이나 전용선 등 안전한 접속 수단 미제공
  - 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관
- 접속기록 보관 및 위 · 변조 방지 조치 위반
  - 개인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력?열람?수정 등 수행업무) 관리 미흡
  - 접속기록을 6개월 이상이 아닌 3개월만 보관

3. 개인정보처리시스템 취약점 진단

관련근거

① 개인정보 보호법 제29조(안전조치의무)
개인정보의 안전성 확보조치 기준 고시 제5조(접근통제)

개인정보처리자는 개인정보의 안전한 저장 및 관리를 위하여 『개인정보의 안전성 확보조치 기준』고시에 따라 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검해야 한다.

중소기업 또는 비영리 단체는 한국인터넷진흥원에서 제공하는 무료 원격 웹 취약점 점검 서비스를 이용해 웹 사이트의 취약점 진단을 수행할 수 있다.

※ 한국인터넷진흥원 웹 취약점 점검 : http://www.krcert.or.kr/kor/webprotect/webprotect_01.jsp)

[표 19] 취약점 진단 시 참고자료

참고자료	웹페이지 주소
OWASP Top 10	https://www.owasp.org/index.php/Top_10_2013-Top_10
SAN Top 25	http://www.sans.org/top25-software-errors/
주요정보통신기반시설 기술적 취약점 분석평가 방법 가이드	http://www.mospa.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000012&nttId=41297
홈페이지 취약점 진단 · 제거 가이드	http://www.kisa.or.kr/public/laws/laws3.jsp

[표 20] 무료 취약점 점검 도구

도구명	도구 위치
Kali Linux	https://www.kali.org/downloads/
Zed Attack Proxy	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
OpenVAS	http://www.openvas.org
Retina CS Community	http://go.beyondtrust.com/cscommunity
Nexpose Community Edition	http://www.rapid7.com/ko/products/nexpose/compare-downloads.jsp
SecureCheq	http://www.tripwire.com/securecheq/
Qualys FreeScan	https://freescan.qualys.com/freescan-front/
Netsparker Community Edition	https://www.netsparker.com/communityedition/
NIKTO	https://cirt.net/nikto2
WIKTO	http://research.sensepost.com/tools/web/wikto

※ 세부 점검 항목은 [별첨 4]『취약점 분석 · 평가 기본항목(웹)』 기준 참고

4. 개인정보처리시스템 접속기록 및 접근권한 점검

관련근거

① 개인정보 보호법 제29조(안전조치의무)
② 정보통신망법 제28조(개인정보의 보호조치)

개인정보취급자가 개인정보가 저장된 DB에 접속하여 개인정보를 열람 · 수정 · 삭제 · 출력 등의 작업을 한 경우 정보주체 식별정보, 개인정보취급자 식별정보, 접속일시, 접속지 정보, 수행업무 등을 기록하고 해당 기록을 반기별 1회이상 정기적으로 확인 및 감독해야 하며 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존 · 관리해야 한다.

단, 정보통신망법상 정보통신서비스제공자는 월 1회 이상 접속기록을 점검하여야 하며, 전기통신사업법상 기간통신사업자의 경우 최소 2년간 접속기록을 보존 · 관리해야 한다.

[표 21] 개인정보처리시스템 접속기록 예시

정보주체 식별정보	취급자 식별정보	접속일시	접속지	수행업무
12345(jykim)	홍길동(HGD)	2014.12.12. 15:00:00	192.168.1.1	조회(고객응대)
6789(shlee)	김갑수(KGS)	2014.12.14. 13:12:34	192.168.1.100	출력(우편발송)

접속기록을 생성하게 되면 아래 표와 같이 생성, 보관, 파기 전반에 걸쳐 안전하게 접속기록을 보관 · 관리하여야 한다.

[표 22] 접속기록 생명주기

시기	내용
생성	개인정보 열람 · 수정 · 삭제 · 출력 등의 작업이 발생한 경우 해당 작업의 식별정보, 접속일시, 접속IP, 수행 업무 등을 기록으로 생성한다.
보관	접속기록을 별도의 DB나 서버 또는 물리적 매체에 안전하게 저장 · 보관해야 하며 이를 위해 필요한 기술적, 물리적 조치를 취해야 한다.
파기	접속기록에 개인정보가 포함되는 경우가 발생할 수 있어 접속기록의 보유 기간이 경과한 경우 로우레벨 포맷 등 프로그램을 이용한 파기나 천공, 파쇄 등의 물리적인 파기 절차를 통해 복구 · 재생할 수 없는 형태로 파기해야 한다.

개인정보처리시스템에 대한 접속기록 유지 · 관리를 위하여 다음 사항을 포함하여 접속기록 관리 방법 및 절차를 수립한다.

주의사항

① 기록 유지·관리가 필요한 주요 접속기록 식별
② 개인정보처리시스템에서 생성되는 접속기록 파일 내용
③ 접속기록 파일의 생성량 및 생성주기
④ 요구되는 보안성에 따른 분석주기
⑤ 접속기록 파일 생성 및 보관정책 등

주의사항

① 물리적 매체에 저장하여 보관하는 경우 접속기록이 위·변조되지 않도록 쓰기 권한을 제한하여 보관하거나 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직하다.

② 접속기록이 위·변조되지 않도록 쓰기 권한을 제한하여 보관하거나 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직하다.

③ 접속기록을 수정 가능한 매체(HDD 또는 테이프)에 백업하는 경우 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 HMAC 값 또는 전자서명 정보를 별도의 매체 또는 관리대장에 보관하는 방법으로 관리할 수 있다.

개인정보처리시스템에 대한 접속기록 저장시 아래와 같은 주의사항을 고려할 수 있도록 한다.

주의사항

① 개인정보처리시스템에 대한 접근권한을 업무 수행 목적에 따라 필요한 최소한의 범위로 업무 담당자에게 차등 부여

② 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소

③ 권한 변경, 부여, 말소 내역을 기록하고 최소 3년간 보관

④ 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급(1인 1계정)하여 책임 추적성 확보

개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 않도록 개인정보처리시스템의 접근권한을 검토하는 등 아래와 같은 안전성 확보에 필요한 조치를 해야 한다.

행정처분 사례

제29조 위반 : 3천만원 이하의 과태료(1회 600만원)

- 세부내용은 시행령 제30조제3항에 따른 '개인정보의 안전성 확보조치 기준' 참조

접근통제 및 접근권한의 제한 조치 위반

- 개인정보취급자의 권한 부여, 변경 또는 말소내역 미기록
- 접근권한의 보관 및 관리 위반
- 홈페이지 관리자 페이지 사용자별 권한차등 미부여, 권한변경 내역 미보관

접속기록 보관 및 위?변조 방지 조치 위반

- 인정보취급자의 시스템 접속기록(식별자, 접속일시, 접속자를 알 수 있는 정보, 입출력?열람?수정 등 수행업무) 관리 미흡
- 접속기록을 6개월 이상이 아닌 3개월만 보관

5. 개인정보 유출 시 통지 및 신고

관련근거

① 개인정보 보호법 제34조(개인정보 유출 통지 등)
② 정보통신망법 제27조의2(개인정보 누출등의 통지·신고)

개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 아래의 사항을 알려야 하며, 1만건 이상 유출시에는 피해확산방지를 위해 행정자치부장관 또는 한국인터넷진흥원에 신고하여야 한다.

주의사항

① 유출된 개인정보의 항목
② 유출된 시점과 그 경우
③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
④ 개인정보처리자의 대응조치 및 피해 구제절차
⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

정보통신망법에 따른 정보통신서비스 제공자등은 개인정보의 분실 · 도난 · 누출 사실을 안 때에 지체 없이 아래의 사항을 포함하여 이용자에게 알리고 24시간 이내에 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.

주의사항

① 누출등이 된 개인정보 항목
② 누출등이 발생한 시점
③ 이용자가 취할 수 있는 조치
④ 정보통신서비스 제공자등의 대응 조치
⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

OO포탈 대응 조치			
한국인터넷진흥원과 협력하여 개인정보 유출 원인을 조사중입니다.			
유출된 개인정보 항목	유출 시점	이용자가 가능한 조치	상담 부서 및 연락처
성명, 주민번호, 성별, 주소	2014.03.01	비밀번호 변경	070-132-1234

[그림 44] 개인정보 유출 시 통지 내용

유출사실을 정보주체에게 통지할 때에는 메일, 서면, 전화 또는 이와 유사한 방법 중 어느 하나를 이용하면 되고 사고에 관한 구체적 내용이 확인되지 않은 경우 현재까지 확인된 내용만 우선 통지할 수 있다. 만일 정당한 사유로 인해 이용자에게 유출 사실을 알리지 못한 경우 각 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 위의 통지를 갈음할 수 있다.

[표 23] 개인정보 유출 표준 통지문안

표준 통지문안 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	〈제목〉 – '유출 통지' 문구 포함
고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 고객님의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	〈사과문〉 – 유출 통지 사실 알림 – 사과문을 먼저 표현
고객님의 개인정보는 2010년 3월 5일 회원관리시스템 장애 처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고, 유지보수업체는 자체 서버에 저장 · 보관하다가 안전한 조치를 다하지 못해 2010년 4월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 서울지방경찰청에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	〈유출된 시점과 경위〉 – 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 – '귀하', '고객님' 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 – 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 등 총 6개입니다.	〈유출된 항목〉 – 유출된 항목을 누락 없이 모두 나열 ※ '등'으로 생략하거나, '회사전화번호' 및 '집전화번호'를 합쳐서 '전화번호'로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	〈개인정보처리자의 대응조치〉 – 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근 통제, 시스템 모니터링 강화 등 조치한 내용 설명
서울지방경찰청이 발표한 수사 결과에 따르면 현재 해커는 검거되었고, 해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다. 따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나, 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다.	〈피해 최소화를 위한 정보주체의 조치방법〉 – 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내 – 사건에 따라 다양한 피해를 추정하여 예방 가능한 방법을 모두 안내(보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구, 감독기관인 0000부 민원신고센터 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	〈개인정보처리자의 피해 구제절차〉 – 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 – 보상이나 배상이 결정되지 않은 경우 계획과 절차를 안내 – 감독기관 등을 통한 구제절차도 안내
앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.	(개인정보처리자의 향후 대응계획) – 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 고객님께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)

표준 통지문안 예시	부가 설명
• 피해 등 접수 담당부서 : 고객지원과 • 피해 등 접수 전화번호 : 02-2345-6789, -9876 • 피해 등 접수 e-메일주소 : abcd@efgh.co.kr	〈피해 등 신고 접수 담당부서 및 연락처〉 - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센타 등 다른 부서를 지정한 경우 해당 부서를 안내
(주)하나둘업체 임직원 일동	(발신명의)

(출처: 개인정보보호종합지원포털 개인정보 유출 시 필수 조치요령 및 표준 통지문안)

※ 부가설명 란에 필수사항은 〈 〉, 참고사항은 ( )로 표기하였음

※ 필수사항이 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

※ 예시를 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

6. 개인정보 이용내역 통지

관련근거

① 정보통신망법 제30조의2(개인정보 이용내역의 통지)

개인정보 이용내역을 통지해야 하는 법적 기준 의무사업장은 아래와 같다.

주의사항

① 정보통신서비스 제공자로서 전년도 말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상
② 정보통신 서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자

※ 정보통신서비스제공자가 아닌 일반사업자는 해당되지 않음

개인정보 이용내역을 통지할 때에는 반드시 아래 사항을 포함하여 전자우편이나 서면, 전화 등 이와 유사한 방법 중 어느 하나의 방법으로 연1회 이상 이용자에게 통지해야 한다.

주의사항

① 개인정보의 수집·이용 목적
② 수집한 개인정보 항목
③ 개인정보를 제공받은 자와 제공 목적(통신비밀보호법 제13조, 제13조의2, 제13조의4 및 전기통신사업법 제83조 제3항에 따른 예외 존재)
④ 취급위탁을 받은 자 및 취급위탁 업무의 내용

◎ 개인정보 이용내역 통지 예시

▶ (수집 · 이용 목적)
⇒ (개인정보 수집 · 이용 목적 기재)
▶ (수집한 개인정보의 항목)
⇒ (수집한 개인정보의 항목 기재)
▶ (개인정보 제3자 제공 관련)
⇒ 개인정보를 제공 받은자 : (개인정보 제공 받은자 기재. 다수일 경우 00등 00사)
⇒ 제공 목적 : (제3자 제공과 관련해서 동의를 받은 목적 중 해당사항 기재)
⇒ 제공한 개인정보 항목 : (제공한 개인정보의 항목 기재)
▶ (개인정보 취급위탁 관련)
⇒ 개인정보의 수탁자 : (개인정보를 취급위탁 받은자 기재. 다수일 경우 00등 00사)
⇒ 취급위탁 목적 : (개인정보 취급위탁 업무 내용 기재)
※ 보다 자세한 사항은 홈페이지를 통해 확인 가능합니다.

※ 개인정보를 제3자 제공이나 취급위탁시 실제로 제공 · 위탁한 내역을 통지하면 됩니다.

(출처: 개정 정보통신망법 개인정보보호 신규제도 안내서, KISA 2012.8)

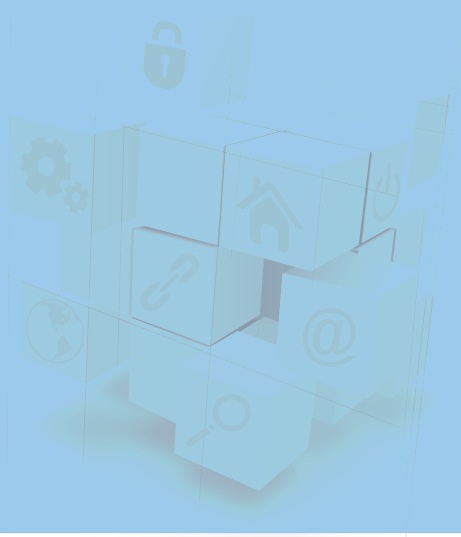
[그림 45] 개인정보 이용내역 통지 예시

제5절 참조문서

- 개인정보 보호법
- 정보통신망법
- 정보통신기반 보호법
- 전자금융거래법
- 표준 개인정보 보호지침(행정안전부고시 제2011-45호)
- 개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)
- 개인정보의 기술적 · 관리적 보호조치 기준(방송통신위원회고시 제2012-50호)
- 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서
- 개인정보보호 종합지원 포털(http://www.privacy.go.kr)
- 개인정보보호 포털(https://www.i-privacy.kr)
- 한국인터넷진흥원(http://www.kisa.or.kr)

별 첨

[별첨 1] 개인정보보호 관련 규정 위반 시 처벌(개인정보 보호법 기준)
[별첨 2] 개인정보보호 관련 규정 위반 시 처벌(정보통신망법 기준)
[별첨 3] 개인정보 처리방침(샘플)(개인정보 보호법 기준)
[별첨 4] 취약점 분석 · 평가 기본항목(웹)
[별첨 5] 개인정보처리시스템 개인정보보호 자가진단 표



별첨 1 개인정보보호 관련 규정 위반 시 처벌(개인정보 보호법 기준)

분류	의무 조치 사항	위반 시 벌칙 규정
수집 및 이용	정보주체의 동의 없는 개인정보 제3자 제공	5년 이하의 징역 또는 5천만원 이하의 벌금
	개인정보의 목적 외 이용 · 제공	
	민감정보 처리기준 위반	
	고유식별정보 처리기준 위반	
	부정한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자	3년 이하의 징역 또는 3천만원 이하의 벌금
	개인정보의 수집기준 위반	5천만원 이하 과태료
	만 14세 미만 아동의 개인정보 수집 시 법정대리인 동의획득의무 위반	
	탈의실 · 목욕실 등 영상정보처리기기 설치 금지 위반	
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자	3천만원 이하 과태료
	최소한의 개인정보 외 정보의 미 동의를 이유로 재화 또는 서비스 제공을 거부한 자	
	주민등록번호를 제공하지 아니할 수 있는 방법 미 제공	
	동의획득방법 위반하여 동의 받은 자	1천만원 이하 과태료
제공 및 위탁	동의 없는 개인정보 제3자 제공	5년 이하의 징역 또는 5천만원 이하의 벌금
	개인정보의 목적 외 이용 · 제공	
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자	3천만원 이하 과태료
	업무위탁 시 공개의무 위반	1천만원 이하 과태료
개인정보 안전관리	주민등록번호 분실, 도난, 유출, 변조 또는 훼손된 경우	5억원 이하 과징금
	개인정보의 누설 또는 타인 이용에 제공	5년 이하의 징역 또는 5천만원 이하의 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자	3년 이하의 징역 또는 3천만원 이하의 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난 · 유출 · 변조 또는 훼손당하거나 분실한 자	2년 이하의 징역 또는 1천만원 이하의 벌금
	안전성 확보에 필요한 조치의무 불이행	3천만원 이하 과태료
	영상정보처리기기 설치 · 운영기준 위반	
	개인정보를 분리해서 저장 · 관리하지 아니한 자	1천만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	

분류	의무 조치 사항	위반 시 벌칙 규정
정보주체 권익 보호	개인정보의 정정 · 삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자	2년 이하의 징역 또는 1천만원 이하의 벌금
	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자	
	개인정보 유출사실 미통지	3천만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한 · 거절	
	정보주체의 정정삭제요구에 따라 필요조치를 취하지 아니한 자	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자	
	시정명령 불이행	
	정보주체의 열람, 정정 · 삭제, 처리정지 요구 거부 시 통지의무 불이행	1천만원 이하 과태료
	관계물품 · 서류 등의 미제출 또는 허위 제출	
	출입 · 검사를 거부 · 방해 또는 기피한 자	
파기	개인정보 미파기	3천만원 이하 과태료

별첨 2 개인정보보호 관련 규정 위반 시 처벌(정보통신망법 기준)

분류	의무 조치 사항	위반 시 벌칙 규정
개인 정보 수집	개인정보 수집 시 다음 사항을 이용자에게 알리고 동의를 받아야 함	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
	① 개인정보의 수집 이용 목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 이용 기간	
	이용자 동의 또는 법률에 특별히 수집 대상 개인정보로 허용된 경우에만 사상, 신념, 과거의 병력(病歷) 등 민감정보 수집 가능	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
	필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스 제공을 거부할 수 없음	• 3천만원 이하의 과태료
	다음의 경우를 제외하고는 이용자의 주민등록번호를 수집 · 이용할 수 없음 ②와 ③의 경우에도 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법을 제공해야 함	• 3천만원 이하의 과태료
	① 본인확인기관으로 지정받은 경우 ② 법령에서 주민등록번호 수집 · 이용을 허용하는 경우 ③ 영업상 목적상 불가피하여 방송통신위원회가 고시하는 경우	
	만14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받아야 함	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
개인 정보 이용, 제공	이용자로부터 동의 받은 목적 등과 다른 목적으로 개인정보 이용 금지	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
	개인정보 제3자 제공시 아래 사항을 이용자에게 알리고 동의를 받아야 함 ※ 요금정산을 위해 필요한 경우와 법률에 특별한 규정이 있는 경우는 예외 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용할 수 없음	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
	① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간	
	제3자 제공에 대한 동의와 개인정보 취급위탁에 대한 동의를 받을 때에는 개인정보 수집 · 이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부할 수 없음	• 1천만원 이하의 과태료
	개인정보 취급위탁 시 아래 사항을 이용자에게 알리고 동의를 받아야 함	• 5년 이하의 징역 또는 5천만원 이하의 벌금 • 위반행위와 관련한 매출액의 3/100 이하 과징금 부과 가능
	① 개인정보 취급위탁을 받는 자 ② 개인정보 취급위탁을 하는 업무의 내용	
	계약을 이행하기 위하여 필요한 경우로서 개인정보 취급방침에 공개하거나 전자우편 등으로 이용자에게 알린 경우에는 예외	• 2천만원 이하의 과태료

분류	의무 조치 사항	위반 시 벌칙 규정
개인 정보 이용, 제공	영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 타인에게 이전하는 경우에는 아래 사항을 인터넷홈페이지 게시, 전자우편 등으로 이용자에게 알려야 함	• 2천만원 이하의 과태료
	① 개인정보를 이전하려는 사실 ② 개인정보를 이전받는 자의 성명(법인의 경우에는 법인의 명칭) · 주소 · 전화번호 및 그 밖의 연락처 ③ 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차	
	영업양수자 등은 당초 제공받은 목적 범위 내에서만 개인정보를 이용하거나 제공할 수 있음	• 5년 이하의 징역 또는 5천만원 이하의 벌금
개인정보 보호조치	개인정보관리책임자 지정	• 2천만원 이하의 과태료
	개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지 첫화면 등에 공개	• 2천만원 이하의 과태료
	개인정보 누출등 사실을 안 때에는 지체 없이 아래의 사항을 해당 이용자에게 알리고 방송통신위원회에 신고해야 함	• 3천만원 이하의 과태료
	① 누출등이 된 개인정보 항목 ② 누출등이 발생한 시점 ③ 이용자가 취할 수 있는 조치 ④ 정보통신서비스 제공자등의 대응 조치 ⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처	
	개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 아래의 기술적 · 관리적 조치를 해야 함 ※ ②~⑤까지의 조치를 하지 아니하여 이용자의 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손한 경우	• 3천만원 이하의 과태료 • 2년 이하의 징역 또는 1천만원 이하의 벌금 • 1억원 이하 과징금 부과 가능
	① 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립 · 시행 ② 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치 · 운영 ③ 접속기록의 위조 · 변조 방지를 위한 조치 ④ 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치 ⑤ 백신 소프트웨어 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치 ⑥ 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치	
	개인정보를 취급하고 있거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손 · 침해 또는 누설하여서는 아니됨 개인정보가 누설된 사정을 알면서 영리 또는 부정한 목적으로 개인정보 제공받는 행위 금지	• 5년 이하의 징역 또는 5천만원 이하의 벌금
정보 파기	수집 · 이용목적 달성, 보유 및 이용기간이 끝난 경우에는 개인정보를 지체없이 파기 이용자가 서비스를 3년 동안 이용하지 아니하는 경우에는 해당 개인정보를 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장 · 관리	• 3천만원 이하의 과태료

분류	의무 조치 사항	위반 시 벌칙 규정
개인 정보 제공, 조치	이용자의 개인정보 열람 또는 제공 요구, 동의철회 시 지체 없이 필요한 조치해야 함 동의철회, 개인정보의 열람 · 제공 또는 오류 정정을 요구하는 방법을 개인정보 수집방법 보다 쉽게 해야 함	• 3천만원 이하의 과태료
	오류 정정을 요구받으면 필요한 조치를 할 때까지 해당 개인정보의 이용 또는 제공 금지	• 5년 이하의 징역 또는 5천만원 이하의 벌금
	수집한 이용자 개인정보의 이용내역(제공 및 개인정보 취급위탁 포함)을 연 1회 이상 이용자에게 통지	• 3천만원 이하의 과태료

별첨 3 개인정보 처리방침(샘플)(개인정보 보호법 기준)

(주)OOO社 개인정보 처리방침

(주)OOO社(이하 '회사'라 한다)는 개인정보 보호법 제30조에 따라 정보주체의 개인정보를 보호하고 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 하기 위하여 다음과 같이 개인정보 처리지침을 수립 · 공개합니다.

제1조(개인정보의 처리목적) 회사는 다음의 목적을 위하여 개인정보를 처리합니다. 처리하고 있는 개인정보는 다음의 목적 이외의 용도로는 이용되지 않으며, 이용 목적이 변경되는 경우에는 개인정보 보호법 제18조에 따라 별도의 동의를 받는 등 필요한 조치를 이행할 예정입니다.

1. 홈페이지 회원 가입 및 관리
   회원 가입의사 확인, 회원제 서비스 제공에 따른 본인 식별 · 인증, 회원자격 유지 · 관리, 제한적 본인확인제 시행에 따른 본인확인, 서비스 부정이용 방지, 만 14세 미만 아동의 개인정보 처리시 법정대리인의 동의여부 확인, 각종 고지 · 통지, 고충처리 등을 목적으로 개인정보를 처리합니다.
2. 재화 또는 서비스 제공
   물품배송, 서비스 제공, 계약서 · 청구서 발송, 콘텐츠 제공, 맞춤서비스 제공, 본인인증, 연령인증, 요금결제 · 정산, 채권추심 등을 목적으로 개인정보를 처리합니다.
3. 고충처리
   민원인의 신원 확인, 민원사항 확인, 사실조사를 위한 연락 · 통지, 처리결과 통보 등의 목적으로 개인정보를 처리합니다.

제2조(개인정보의 처리 및 보유기간) ① 회사는 법령에 따른 개인정보 보유 · 이용기간 또는 정보주체로부터 개인정보를 수집시에 동의받은 개인정보 보유 · 이용기간 내에서 개인정보를 처리 · 보유합니다.

② 각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.

1. 홈페이지 회원 가입 및 관리 : 사업자/단체 홈페이지 탈퇴시까지
   다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지
   1) 관계 법령 위반에 따른 수사 · 조사 등이 진행중인 경우에는 해당 수사 · 조사 종료시까지
   2) 홈페이지 이용에 따른 채권 · 채무관계 잔존시에는 해당 채권 · 채무관계 정산시까지
2. 재화 또는 서비스 제공 : 재화 · 서비스 공급완료 및 요금결제 · 정산 완료시까지
   다만, 다음의 사유에 해당하는 경우에는 해당 기간 종료시까지
   1) 「전자상거래 등에서의 소비자 보호에 관한 법률」에 따른 표시 · 광고, 계약내용 및 이행 등 거래에 관한 기록
      – 표시 · 광고에 관한 기록 : 6월
      – 계약 또는 청약철회, 대금결제, 재화 등의 공급기록 : 5년
      – 소비자 불만 또는 분쟁처리에 관한 기록 : 3년
   2) 「통신비밀보호법」제41조에 따른 통신사실확인자료 보관
      – 가입자 전기통신일시, 개시 · 종료시간, 상대방 가입자번호, 사용도수, 발신기지국 위치추적자료 : 1년

– 컴퓨터통신, 인터넷 로그기록자료, 접속지 추적자료 : 3개월

제3조(개인정보의 제3자 제공) ① 회사는 정보주체의 개인정보를 제1조(개인정보의 처리 목적)에서 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등 개인정보 보호법 제17조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.

② 회사는 다음과 같이 개인정보를 제3자에게 제공하고 있습니다.

– 개인정보를 제공받는 자 : (주) OOO 카드

– 제공받는 자의 개인정보 이용목적 : 이벤트 공동개최 등 업무제휴 및 제휴 신용카드 발급

– 제공하는 개인정보 항목 : 성명, 주소, 전화번호, 이메일주소, 카드결제계좌정보, 신용도정보

– 제공받는 자의 보유 · 이용기간 : 신용카드 발급계약에 따른 거래기간동안

제4조(개인정보처리의 위탁) ① 회사는 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

1. 전화 상담센터 운영

– 위탁받는 자 (수탁자) : OOO 컨택센터

– 위탁하는 업무의 내용 : 전화상담 응대, 부서 및 직원 안내 등

2. A/S 센터 운영

– 위탁받는 자 (수탁자) : OOO 전자

– 위탁하는 업무의 내용 : 고객 대상 제품 A/S 제공

② 회사는 위탁계약 체결시 개인정보 보호법 제25조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적 · 관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리 · 감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다.

③ 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

제5조(정보주체의 권리 · 의무 및 행사방법) ① 정보주체는 회사에 대해 언제든지 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다.

1. 개인정보 열람요구
2. 오류 등이 있을 경우 정정 요구
3. 삭제요구
4. 처리정지 요구

② 제1항에 따른 권리 행사는 회사에 대해 서면, 전화, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며 회사는 이에 대해 지체없이 조치하겠습니다.

③ 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 회사는 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않습니다.

④ 제1항에 따른 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수 있습니다. 이 경우 개인정보 보호법 시행규칙 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

⑤ 정보주체는 개인정보 보호법 등 관계법령을 위반하여 회사가 처리하고 있는 정보주체 본인이나 타인의 개인정보 및 사생활을 침해하여서는 아니됩니다.

제6조(처리하는 개인정보 항목) 회사는 다음의 개인정보 항목을 처리하고 있습니다.

1. 홈페이지 회원 가입 및 관리
   • 필수항목 : 성명, 생년월일, 아이디, 비밀번호, 주소, 전화번호, 성별, 이메일주소, 아이핀번호
   • 선택항목 : 결혼여부, 관심분야
2. 재화 또는 서비스 제공
   • 필수항목 : 성명, 생년월일, 아이디, 비밀번호, 주소, 전화번호, 이메일주소, 아이핀번호, 신용카드번호, 은행계좌정보 등 결제정보
   • 선택항목 : 관심분야, 과거 구매내역
3. 인터넷 서비스 이용과정에서 아래 개인정보 항목이 자동으로 생성되어 수집될 수 있습니다.
   • IP주소, 쿠키, MAC주소, 서비스 이용기록, 방문기록, 불량 이용기록 등

제7조(개인정보의 파기) ① 회사는 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기합니다.

② 정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차
   회사는 파기 사유가 발생한 개인정보를 선정하고, 회사의 개인정보 보호책임자의 승인을 받아 개인정보를 파기합니다.
2. 파기방법
   회사는 전자적 파일 형태로 기록 · 저장된 개인정보는 기록을 재생할 수 없도록 로우레벨포멧(Low Level Format) 등의 방법을 이용하여 파기하며, 종이 문서에 기록 · 저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

제8조(개인정보의 안전성 확보조치) 회사는 개인정보의 안전성 확보를 위해 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치 : 내부관리계획 수립 · 시행, 정기적 직원 교육 등
2. 기술적 조치 : 개인정보처리시스템 등의 접근권한 관리, 접근통제시스템 설치, 고유식별정보 등의 암호화, 보안프로그램 설치
3. 물리적 조치 : 전산실, 자료보관실 등의 접근통제

제9조(개인정보 보호책임자) ① 회사는 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호책임자
성명 : OOO
직책 : OOO 이사
연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉
※ 개인정보 보호 담당부서로 연결됩니다.

▶ 개인정보 보호 담당부서
부서명 : OOO 팀
담당자 : OOO

연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

② 정보주체께서는 회사의 서비스(또는 사업)을 이용하시면서 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의하실 수 있습니다. 회사는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

제10조(개인정보 열람청구) 정보주체는 개인정보 보호법 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. 회사는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

▶ 개인정보 열람청구 접수 · 처리 부서

부서명 : OOO

담당자 : OOO

연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

제11조(권익침해 구제방법) 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의하실 수 있습니다.

〈아래의 기관은 회사와는 별개의 기관으로서, 회사의 자체적인 개인정보 불만처리, 피해구제 결과에 만족하지 못하시거나 보다 자세한 도움이 필요하시면 문의하여 주시기 바랍니다〉

▶ 개인정보 침해신고센터 (한국인터넷진흥원 운영)

– 소관업무 : 개인정보 침해사실 신고, 상담 신청

– 홈페이지 : privacy.kisa.or.kr

– 전화 : (국번없이) 118

– 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 개인정보 분쟁조정위원회 (한국인터넷진흥원 운영)

– 소관업무 : 개인정보 분쟁조정신청, 집단분쟁조정 (민사적 해결)

– 홈페이지 : privacy.kisa.or.kr

– 전화 : (국번없이) 118

– 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 대검찰청 사이버범죄수사단 : 02-3480-3573 (www.spo.go.kr)

▶ 경찰청 사이버테러대응센터 : 1566-0112 (www.netan.go.kr)

제12조(영상정보처리기기 설치 · 운영) ① 〈사업자/단체명〉 은(는) 아래와 같이 영상정보처리기기를 설치 · 운영하고 있습니다.

1. 영상정보처리기기 설치근거 · 목적 : 〈사업자/단체명〉 의 시설안전 · 화재예방
2. 설치 대수, 설치 위치, 촬영 범위 : 사옥 로비 · 전시실 등 주요시설물에 00대 설치, 촬영범위는 주요시설물의 전 공간을 촬영
3. 관리책임자, 담당부서 및 영상정보에 대한 접근권한자 : OOO 팀 OOO 과장
4. 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
   – 촬영시간 : 24시간 촬영
   – 보관기간 : 촬영시부터 30일
   – 보관장소 및 처리방법 : OOO팀 영상정보처리기기 통제실에 보관 · 처리
5. 영상정보 확인 방법 및 장소 : 관리책임자에 요구 (OOO팀)

6. 정보주체의 영상정보 열람 등 요구에 대한 조치 : 개인영상정보 열람 · 존재확인 청구서로 신청하여야 하며, 정보주체 자신이 촬영된 경우 또는 명백히 정보주체의 생명 · 신체 · 재산 이익을 위해 필요한 경우에 한해 열람을 허용함
7. 영상정보 보호를 위한 기술적 · 관리적 · 물리적 조치 : 내부관리계획 수립, 접근통제 및 접근권한 제한, 영상정보의 안전한 저장 · 전송기술 적용, 처리기록 보관 및 위 · 변조 방지조치, 보관시설 마련 및 잠금장치 설치 등

제13조(개인정보 처리방침 변경) ① 이 개인정보 처리방침은 20XX. X. X부터 적용됩니다.

② 이전의 개인정보 처리방침은 아래에서 확인하실 수 있습니다.

- 20XX. X. X ~ 20XX. X. X 적용 (클릭)
- 20XX. X. X ~ 20XX. X. X 적용 (클릭)

별첨 4 취약점 분석 · 평가 기본항목(웹)

코드	취약점명	설 명	등급
BO	버퍼오버플로우	메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점	상
FS	포맷스트링	스트링을 처리하는 부분에서 메모리 공간에 접근할 수 있는 문제를 이용하는 취약점	상
LI	LDAP인젝션	LDAP(Lightweight Directory Access Protocol) 쿼리를 주입함으로서 개인정보 등의 내용이 유출될 수 있는 문제를 이용하는 취약점	상
OC	운영체제명령실행	웹사이트의 인터페이스를 통해 웹서버를 운영하는 운영체제 명령을 실행하는 취약점	상
SI	SQL인젝션	SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점	상
SS	SSI인젝션	SSI(Server-side Include)는 "Last modified"와 같이 서버가 HTML 문서에 입력같는 변수 값으로, 웹서버상에 있는 파일을 include 시키고, 명령문이 실행되게 하여 데이터에 접근할 수 있는 취약점	상
XI	XPath인젝션	조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점	상
DI	디렉토리인덱싱	요청 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점	상
IL	정보누출	웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있는 취약점	상
CS	악성콘텐츠	웹애플리케이션에 정상적인 컨텐츠 대신에 악성 컨텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점	상
XS	크로스사이트스크립팅	웹애플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	상
BF	약한문자열강도	사용자의 이름이나 패스워드, 신용카드 정보나 암호화 키 등을 자동으로 대입하여 여러 시행착오 후에 맞는 값이 발견되는 취약점	상
IA	불충분한 인증	민감한 데이터에 접근할 수 있는 곳에 취약한 인증 메커니즘으로 구현된 취약점	상
PR	취약한 패스워드 복구	취약한 패스워드 복구 메커니즘(패스워드 찾기 등)에 대해 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경, 복구할 수 있는 취약점	상
CF	크로스사이트 리퀘스트변조(CSRF)	CSRF 공격은 로그온한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹애플리케이션에 전송하는 취약점	상
SE	세션 예측	단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 식별자(ID)를 예측하여 세션을 가로챌 수 있는 취약점	상
IN	불충분한 인가	민감한 데이터 또는 기능에 대한 접근권한 제한을 두지 않은 취약점	상
SC	불충분한 세션만료	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점	상
SF	세션고정	세션값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점	상
AU	자동화공격	웹애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점	상
PV	프로세스검증누락	공격자가 응용의 계획된 플로우 통제를 우회하는 것을 허가하는 취약점	상
FU	파일업로드	파일을 업로드 할 수 있는 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점	상
FD	파일다운로드	파일 다운로드 스크립트를 이용하여 첨부된 주요 파일을 다운로드 할 수 있는 취약점	상
AE	관리자페이지 노출	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점	상
PT	경로추적	공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행할 수 있는 취약점	상
PL	위치공개	예측 가능한 디렉토리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점	상
SN	데이터평문전송	서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점	상
CC	쿠키변조	적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점	상

(출처: 주요정보통신기반시설 취약점 분석 · 평가 기준, 미래창조과학부, 2013.8.8.)

별첨 5 개인정보처리시스템 개인정보보호 자가진단 표

단계	분야	점검사항
수집단계	수집제한	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 목적 내에서만 개인정보를 수집하도록 개발하였는가?
	정보주체 동의	개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체의 동의를 얻은 후에 수집하도록 개발하였는가?
	법정대리인 동의 및 고지	만14세 미만의 아동의 개인정보를 수집 할 경우 법정대리인에게 필요한 사항을 고지하고 동의하도록 개발하였는가?
	민감정보 및 고유식별정보 수집제한	정보주체의 권리 이익이나 사생활을 뚜렷하게 침해할 우려가 있거나, 그 자체로 개인을 식별할 수 있는 고유식별정보는 수집하지 않아야 하며, 필요한 경우 정보 주체로부터 별도의 동의를 받도록 개발하였는가?
	대체가입수단 제공	인터넷 홈페이지 회원가입 시 주민등록번호에 대한 대체가입 수단을 제공하도록 개발하였는가?
	개인정보처리방침 수립 및 공개	개인정보 처리방침을 수립하여 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하였는가?
이용단계	제3자 제공	개인정보를 제3자에게 제공 시 정보주체로부터 동의를 받은 후에 개인 정보에 대한 적절한 보호조치 및 3자 제공을 하도록 개발하였는가?
	목적 외 이용	개인정보는 정보주체에게 고지하고 동의 받은 범위를 벗어나 이용 및 제공하지 않도록 개발하였는가?
	개인정보 최신화	처리하고 있는 개인정보는 정확성, 완전성, 최신성을 유지할 수 있도록 정보주체가 언제든지 확인하고 변경 가능하도록 개발하였는가?
	접속기록관리	개인정보처리시스템에 대한 접속기록 및 권한변경에 대해 로그를 남기고 이를 안전하게 백업관리 되도록 개발하였는가?
파기단계	파기 기록 관리	개인정보처리자는 개인정보의 파기에 관한 사항을 기록 관리되도록 개발하였는가?
	개인정보 완전 파기	개인정보처리자는 개인정보 파기에 관한 관리 계획을 수립하고, 관리계획에 따라 개인정보의 수집 목적이 달성된 경우, 개인정보를 안전한 방법으로 지체 없이 완전 파기되도록 개발하였는가?
	개인정보 보관	개인정보를 파기하기 전 일정기간 보관을 해야 하는 경우에는 기존 개인정보와 분리된 영역에 저장하고 접근을 통제하는 등의 방법이 적용되도록 개발하였는가?

(참고자료 : 개인정보수준진단표, PIPL인증기준, PIMS준 등)

별첨 6 개인정보의 안전성 확보조치 기준(개정 2014.12.30.)

개인정보의 안전성 확보조치 기준

제정 2011. 9.30. 행정안전부고시 제2011-43호
개정 2014.12.30. 행정자치부고시 제2014- 7호

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "소상공인"이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」제2조에 해당하는 자를 말한다.
5. "중소사업자"란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.
7. "개인정보취급자"란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.
9. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
10. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
11. "내부관리계획"이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립 · 시행하는 내부 기준을 말한다.
12. "비밀번호"라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자,

접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.
17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

제3조(내부관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가

상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제9조(물리적 접근 방지) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.
② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출 · 입 통제를 위한 보안대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

부칙〈제2011-43호, 2011. 9. 30.〉

제1조 이 기준은 고시한 날부터 시행한다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치 · 운영 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙〈제2014-7호, 2014. 12. 30.〉

이 기준은 고시한 날부터 시행한다.

별첨 7 개인정보처리시스템 구축 · 운영시 이용 가능한 공개 소프트웨어

종류	이름	다운로드 주소
방화벽	smoothwall	http://www.smoothwall.org/download/
	pfSense	https://www.pfsense.org/download/
	endian	http://www.endian.com/en/community/download/#.VKqulyusVrM
IPS/IDS	Snort	https://www.snort.org/downloads
	Suricata	http://suricata-ids.org/download/
웹방화벽	캐슬	http://www.krcert.or.kr/kor/webprotect/webprotect_03.jsp
	WebKnight	http://www.aqtronix.com/?PageID=136
	ModSecurity	http://www.modsecurity.org/download.html
웹쉘탐지	휘슬	http://www.krcert.or.kr/kor/webprotect/webprotect_02.jsp
SSL/TLS	OpenSSL	https://www.openssl.org/source/
SSH	OpenSSH	http://www.openssh.com/
VPN	OpenVPN	https://openvpn.net/index.php/open-source/downloads.html
암호화	SEED	http://seed.kisa.or.kr/iwt/ko/sup/EgovSeedInfo.do
	ARIA	http://seed.kisa.or.kr/iwt/ko/bbs/EgovReferenceList.do?bbsId=BBSMSTR_000000000002
	HIGHT	
	SHA-256	
	Beecrypt	http://sourceforge.net/projects/beecrypt/files/latest/download
완전삭제	Eraser	http://www.tolvanen.com/eraser/download
	SDelete	http://technet.microsoft.com/ko-kr/sysinternals/bb897443(en-us).aspx
	BitKiller	http://sourceforge.net/projects/bitkiller/

제2차 개정

공공기관 영상정보처리기기 설치·운영 가이드라인

2015. 1. 12.

행 정 자 치 부

본 가이드라인은 개인정보 보호법 제25조, 같은 법 시행령 제22조부터 제27조까지 및 표준개인정보 보호지침 제3장의 내용을 설명한 것입니다.

본 가이드라인은 2012년 3월 5일 제정하고, 2012년 12월 1일 1차 개정한 바 있으며, 일부 수정사항을 반영하여 2차 개정, 2015년 1월 12일부터 시행합니다.

주요 개정사항

○ 공개·비공개된 장소 추가·보완

○ 안내판 설치 장소 구체화

○ 영상정보 보관 및 파기, 위수탁 내용 보완

○ 제공 시 준수사항 및 절차 구체화 등

목 차

제1장 개 요

1. 제정 목적
2. 용어 정의
3. 기본원칙 및 주요내용

제2장 항목별 세부내용

1. 영상정보처리기기 설치·운영 제한
2. 사생활침해 우려 장소 설치·운영 금지
3. 임의조작·녹음 금지
4. 영상정보처리기기 설치 시 의견 수렴
5. 안내판의 설치
6. 영상정보처리기기 운영·관리 방침 수립
7. 관리책임자의 지정
8. 영상정보의 목적 외 이용 및 제3자 제공
9. 보관 및 파기
10. 영상정보처리기기 설치·운영 사무의 위탁
11. 열람등의 청구
12. 개인영상정보의 안전성 확보를 위한 조치
13. 개인영상정보처리기기의 설치·운영에 대한 점검

제1장 개요

1. 제정 목적

이 가이드라인은 공공기관의 영상정보처리기기 설치·운영 및 개인영상정보 보호에 대하여 공공기관이 준수하여야 할 사항을 업무담당자가 쉽게 이해할 수 있도록 기준을 제시함을 목적으로 합니다.

2. 용어 정의

○ “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로써 시행령 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 의미합니다.(법 제2조제7호, 시행령 제3조)

※ 본 가이드라인에서, 「개인정보 보호법」은 ‘법’, 「개인정보 보호법」 시행령은 ‘시행령, 「개인정보 보호법」 시행규칙은 ‘시행규칙, 「표준 개인정보 보호지침」은 ‘표준지침’으로 표기함

1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치
   가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
   나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라: 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

○ “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 의미합니다.(표준지침 제2조제9호)

○ “영상정보처리기기운영자”라 함은 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 의미합니다.

※ 법 제25조제1항에 따라 영상정보처리기기를 설치·운영하는 자가 아닌 경우(비공개 장소에 설치된 영상정보처리기기)에는「개인정보 보호법」상 “개인정보처리자”임

○ “공개된 장소”란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 다수(정보주체)가 접근 및 통행하는 데에 제한을 받지 아니하는 장소를 의미합니다.

○ “비공개된 장소”인 경우에는 법 제15조제1항에 따라 정보주체의 동의나 다음과 같이 법률에 특별한 규정이 있는 경우 등에만 영상정보처리기기의 설치·운영(개인영상정보의 수집 및 이용)이 가능합니다.

[‘법률에 특별한 규정이 있는 경우’의 예]

- 「근로자참여 및 협력증진에 관한 법률」제20조제1항제14호
  - 사업장 내 근로자 감시 설비의 설치는 노사협의회의 협의사항
- 「초·중등교육법」제30조의8
  - 학교의 장은 학생의 안전을 위하여 영상정보처리기기 설치에 관한 사항을 시행해야함

[참고] “공개된 장소”의 예시

- 도로, 공원, 공항, 항만, 주차장, 놀이터, 지하철역 등의 공공장소
- 백화점, 대형마트, 상가, 놀이공원, 극장 등 시설
- 버스, 택시 등 누구나 탑승할 수 있는 대중교통
- 병원 대기실, 접수대, 휴게실
- 구청·시청·주민센터의 민원실 등 국가 또는 지방자치단체가 운영하는 시설로 민원인 또는 주민의 출입에 제한이 없는 공공기관 내부

[참고] "비공개된 장소"의 예시

- 입주자만 이용 가능한 시설, 직원만 출입이 가능한 사무실, 권한이 있는 자만 접근 가능한 통제구역
- 학생, 교사 등 학교관계자만 출입이 가능한 학교시설(교실, 실험실 등)
- 진료실, 입원실, 수술실, 비디오 감상실, 노래방의 개별 방, 지하철 내 수유실 등 사생활 침해 위험이 큰 공간

【Q】 사무실은 공개된 장소인지?

A. 출입이 통제되어 해당 사무실에 직원 등 특정한 사람만 들어갈 수 있다면 공개된 장소로 볼 수 없습니다.

사무실이라고 하더라도 출입이 통제되지 않아 민원인이나 불특정 다수인이 아무런 제약 없이 출입이 가능하다면 공개된 장소에 해당합니다.

【Q】 출입이 통제되는 사무실에 CCTV를 설치하는 경우?

A. 비공개된 장소에 설치된 영상정보처리기기는 법 제25조가 적용되지 않으나 이를 통해 수집되는 영상정보는 개인정보에 해당하므로 법 제15조가 적용됩니다.

특정인에 한하여 출입할 수 있는 사무실 등 비공개된 장소에 영상정보처리기기를 설치하고자 하는 경우에는 촬영 범위에 포함된 모든 정보주체의 동의를 받는 것이 바람직하며, 안내판 설치나 보호조치 등은 공개된 장소에 설치된 영상정보처리기기 규정을 준용하는 것을 권장합니다.

【Q】 외부를 촬영하는 차량용 블랙박스가 영상정보처리기기인지?

A. 영상정보처리기기는 일정한 공간에 지속적으로 설치되어 해당 공간을 지속적으로 촬영(촬영의 지속성)하는 것을 말하므로, 차량 외부를 촬영하는 블랙박스는「개인정보 보호법」상 영상정보처리기기에 해당하지 않습니다.

다만, 차량에 설치되어 차량 내부를 촬영하는 CCTV는 차량 내부라는 일정한 공간을 지속적으로 촬영하는 것으로「개인정보 보호법」상 영상정보처리기기에 해당합니다.

3. 기본원칙 및 주요내용

영상정보처리기기를 설치·운영하려는 공공기관은 개인의 사생활이 침해되지 않도록 영상정보처리기기를 최소한으로 설치·운영하여야 하며, 개별 구체적 사안에서 아래의 각 원칙이 구현될 수 있도록 적용·운영하여야 함

- ○ 영상정보처리기기 설치·운영 제한 및 필요 최소한 촬영 (항목별 세부내용 1,2 참조)
- ○ 영상정보처리기기 임의조작·녹음 금지 (항목별 세부내용 3 참조)
- ○ 설치 시 의견수렴 및 안내판 설치를 통한 설치 사실 공지 (항목별 세부내용 4,5 참조)
- ○ 영상정보처리기 운영·관리 방침 수립·공개 및 책임자 지정 (항목별 세부내용 6,7 참조)
- ○ 영상정보의 목적 외 이용·제공 제한 및 보관·파기 철저 (항목별 세부내용 8,9 참조)
- ○ 영상정보처리기기의 설치·운영 위탁 시 관리·감독 철저 (항목별 세부내용 10 참조)
- ○ 정보주체의 자기영상정보 열람권 보장 (항목별 세부내용 11 참조)
- ○ 개인영상정보의 안전성 확보 조치 및 자체 점검 현황 등록 (항목별 세부내용 12,13 참조)

제2장 항목별 세부내용

1. (영상정보처리기기 설치·운영 제한) 누구든지 공개된 장소에 영상정보처리기기를 설치·운영하는 것은 원칙적으로 금지되며 다른 법익의 보호를 위하여 필요한 경우 예외적으로 설치·운영이 허용됨

○ 공개된 장소에서의 영상정보처리기기 설치는 원칙적으로 금지되고, 예외적으로 법 제25조에서 정하는 사유에 해당하는 경우에만 영상정보처리기기를 설치·운영할 수 있습니다.(법 제25조제1항)

영상정보처리기기 설치·운영 허용

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

○ 영상정보처리기기는 개인의 의사와 무관하게 초상 및 활동 정보가 수집되어 무단 공개나 유출 등으로 인한 사생활 침해 우려가 높은 만큼 영상정보처리기기임을 쉽게 인식할 수 있는 형태의 영상정보처리기기를 정보주체 눈에 잘 띄는 곳에 설치·운영하는 것이 바람직합니다.

○ 개인정보의 최소 수집원칙에 따라 영상정보처리기기의 설치목적을 달성할 수 있는 최소한의 범위(촬영장소, 촬영각도 및 시간) 내에서 개인정보를 수집해야 합니다.(법 제3조제1항)

2. (사생활침해 우려 장소 설치·운영 금지) 불특정 다수가 이용하는 공개된 장소라도 현저히 사생활 침해 우려가 있는 장소는 영상정보처리기기 설치·운영이 금지됨

○ 개인의 신체를 노출시킬 우려가 있는 목욕실, 화장실, 발한실(發汗室), 탈의실, 기타 신체의 노출 외에도 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하는 행위는 금지됩니다.(법 제25조제2항)

【Q】 범죄 예방 및 시설안전을 확인하기 위하여 민원실의 화장실 내부에 CCTV를 설치할 수 있는지?

A. 어떤 목적으로든 화장실 등 사생활침해 우려 장소에 CCTV를 설치할 수 없습니다. 또한 외부에 설치하였더라도 화장실 등 사생활침해 우려 장소의 내부가 촬영되도록 설치하여서는 아니 됩니다.

○ 다만, 교도소, 정신보건시설 등과 같이 법령에 근거하여 사람을 보호하는 시설로서 대통령령으로 정한 시설에 대해서는 예외적으로 영상정보처리기기를 설치·운영 할 수 있습니다.(법 제25조제2항)

※ 개별 법령상 특별한 절차가 있는 경우 이에 따라야 함

개인의 사생활을 현저히 침해할 우려가 있는 장소의 예외적 설치·운영 허용

1. 「형의 집행 및 수용자의 처우에 관한 법률」 제2조제4호에 따른 교정시설(교도소·구치소 및 그 지소)
2. 「정신보건법」 제3조제3호부터 제5호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당), 정신질환자사회복귀시설, 정신요양시설

3. (임의조작·녹음 금지) 영상정보처리기기에는 녹음 기능을 사용할 수 없고, 설치 목적과 다른 목적으로 임의 조작할 수 없음

○ 영상정보처리기기운영자는 녹음 기능을 사용할 수 없습니다.(법 제25조제5항)

【Q】 교통단속과 위반행위 처분을 하는 부서인데, 민원인의 폭언·폭행 방지를 위하여 CCTV를 설치하고 녹음도 할 수 있는지?

A. 공공기관의 사무실이라도 민원인이 자유롭게 출입하는 공간은 공개된 장소에 해당하며, 이 경우 법 제25조에 따라 CCTV를 설치할 수 있습니다. 하지만 어떤 목적으로든 CCTV를 통한 녹음은 금지됩니다.

○ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비출 수 없습니다. (법 제25조제5항)

【Q】 민원실에 설치한 CCTV로 방문기록 등을 촬영할 수 있는지?

A. 공개된 민원실에는 범죄예방 등의 목적으로만 CCTV를 설치할 수 있는 바, 방문기록을 촬영하기 위해 CCTV를 설치하는 것은 법으로 금지되어 있고, 기존 CCTV로 방문기록을 위해 촬영하는 것은 설치 목적을 벗어난 촬영이므로, 이 경우 촬영 각도를 조절해야 합니다.

【Q】 영상정보처리기기의 줌(Zoom) 기능이나 촬영방향 전환 기능을 이용할 수 있는지?

A. 영상정보처리기기를 당초 설치 목적이 아닌 다른 목적으로 임의로 조작하거나 다른 곳을 촬영하는 것을 금지하는 것으로, 당초 설치 목적 범위 내에서 이용하는 것은 가능합니다.

4. (영상정보처리기기 설치 시 의견 수렴) 공개된 장소 및 교도소·정신보건시설 등 대통령령으로 정한 장소에 영상정보처리기기를 설치·운영하려는 공공기관의 장은 관계 전문가 및 이해관계인의 의견을 수렴하여야 함

○ 공공기관은 영상정보처리기기 설치·운영 시 다음 중 어느 하나에 해당하는 절차를 거쳐 관계인의 의견을 수렴하여 반영하여야 합니다.(법 제25조제3항)

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견 청취(공청회 등)
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

【Q】 공익목적으로 CCTV를 설치할 경우 행정자치부와 사전 협의를 하여야 하는지?

A. 구 「공공기관의 개인정보 보호에 관한 법률」에서는 개인정보파일 보유 시 사전 협의를 하게 되어 있었으나, 「개인정보 보호법」에서는 사전 협의 제도를 두고 있지 않으므로, 관계인의 의견 수렴 절차를 거쳐 설치할 수 있습니다.

다만, 공공기관의 장은 영상정보처리기기 관련 지침의 준수 여부에 대한 자체점검을 실시하여 매년 3월 31일까지 그 결과를 행정자치부 장관에게 통보하고 개인정보보호종합지원시스템(http://intra.privacy.go.kr)에 등록하여야 합니다.

○ 영상정보처리기기의 설치 목적 변경 및 추가 설치 등의 경우에도 관계 전문가 및 이해관계인의 의견을 수렴하여야 합니다. 다만 동일 목적 내 단순히 추가적으로 설치하는 경우에는 의견 수렴을 하지 않을 수 있습니다.(표준지침 제42조)

[통합관리를 위한 목적사항 추가 시 절차]
1. 목적 변경에 따른 관계 전문가 및 이해관계인의 의견 수렴
2. 안내판에 추가된 설치 목적 및 통합관리에 관한 내용을 기재

※ 기존 영상정보처리기기의 설치목적 사항 변경, 통합관리를 위한 목적 추가 등

○ 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설에 영상정보처리기기를 설치하는 경우 다음 각 호에 해당하는 사람으로부터 의견을 수렴하여야 합니다.(법 제25조제3항)

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

5. (안내판의 설치) 공공기관의 장은 영상정보처리기기 설치 시 정보주체가 쉽게 알아볼 수 있도록 안내판을 설치하여야 함

○ 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 설치하며 안내판의 크기나 위치는 자율적으로 정하되, 정보주체가 손쉽게 인식할 수 있도록 다음 사항을 유의하여 설치하여야 합니다.(법 제25조제4항, 시행령 제24조제1항)

1. 안내판은 정보주체가 쉽게 알아볼 수 있는 출입구, 정문 등 눈에 잘 띄는 장소에 설치해야 함
2. 건물 내, 공원 등 설치 장소에 따라 정보주체가 쉽게 판독할 수 있도록 안내판의 글자 크기와 높이를 조절하여 설치해야 함

[참고] 안내판 설치 장소의 예시

- 건물 : 건물 1층 출입구 또는 정문, 기타 사람들의 이동이 빈번한 각 층의 출입구, 안내데스크 등 눈에 잘 띄는 곳
- 건물외의 장소(공원 등) : 각 출입구, 기둥 또는 시설물 등 눈에 잘 띄는 곳
- 상가 : 주(主)출입문, 계산대 등 눈에 잘 띄는 곳
- 버스 등 대중교통 : 승하차 출입문, 버스내 노선도 옆 등 승객의 눈에 잘 띄는 곳
- 택시 : 보조석 앞, 좌석 머리받침 뒤편 등 승객의 눈에 잘 띄는 곳
- 주차장 : 입구, 정산소, 주차장 내 기둥 등 눈에 잘 띄는 곳

○ 특히, 외국인이 자주 이용하는 장소인 경우, 안내판은 한국어와 외국어로 병기하는 것이 바람직합니다.

○ 영상정보처리기기의 설치·운영을 위탁한 경우에는 영상정보처리기기 위탁자의 관리책임자와 더불어 수탁관리자의 성명(또는 직책)·업체명 및 연락처를 함께 기재하여야 합니다.(시행령 제26조제2항, 표준지침 제47조제1항)

안내판에 기재하여야 할 사항

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명(또는 직책) 및 연락처
4. (영상정보처리기기 설치·운영을 위탁한 경우) 수탁관리자 성명(또는 직책)·업체명 및 연락처

○ 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치 지역임을 표시하는 안내판을 설치할 수 있습니다.(시행령 제24조제1항)

※ 주차장 등과 같이 건물 주(主)출입문과 동선이 분리된 장소에는 출입구 마다 안내판을 부착하는 것이 바람직합니다.

○ 영상정보처리기기의 효율적 관리와 정보 연계를 위하여 통합 관리하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 안내판에 기재하여야 합니다.(표준지침 제43조제3항)

○ 영상정보처리기기운영자가 서로 다른 경우에는 동일한 장소 또는 건물이라고 하더라도 영상정보처리기기운영자 별로 안내판을 각각 설치하여야 합니다.

○ 다음에 해당하는 경우에는 안내판 설치를 갈음하여 해당 공공기관의 인터넷 홈페이지에 안내판에 기재하여야 할 사항을 게재할 수 있습니다. (시행령 제24조제2항·제3항)

※ 홈페이지가 없는 경우 관보 또는 해당 공공기관 소재지에서 시·도 이상의 지역을 주된 보급지역으로 하는 일반일간신문, 일반주간신문 등에 게재 가능

1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판 설치가 불가능하거나 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우

<안내판 및 홈페이지 게재 내용 예시>

CCTV 설치 안내

◈ **설치목적 : 범죄 예방 및 시설안전**
◈ **설치장소 : 출입구의 벽면/천장, 엘리베이터/ 각층의 천장**
◈ **촬영범위 : 출입구, 엘리베이터 및 각층 복도(360° 회전)**
◈ **촬영시간 : 24시간 연속 촬영**
◈ **관리책임자 : 0000과 홍길동 (02-000-0000)**
(설치·운영을 위탁한 경우)
◈ **수탁관리자 : 0000업체 박길동 (02-000-0000)**

※ 안내판에 CCTV 그림을 표시하여 정보주체가 쉽게 인식할 수 있도록 하는 것이 바람직합니다.

○ 다음에 해당하는 시설에 설치하는 영상정보처리기기에 대해서는 안내판을 설치하지 않을 수 있습니다.(시행령 제24조제4항)

1. 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설
2. 「통합방위법」 제2조제13호에 따른 국가중요시설
3. 「보안업무규정」 제36조에 따른 보안목표시설

【Q】 보안목표시설인 공공기관의 민원실에는 CCTV 안내판을 설치하지 않아도 되는지?

A. 보안목표시설인 경우에는 안내판을 부착하지 않을 수도 있습니다. 하지만, 민원인들이 출입하는 민원실의 경우 공개된 장소로 민원인의 자기정보결정권 보장 등을 위해 안내판을 부착하는 것이 바람직합니다.

6. (영상정보처리기기 운영·관리 방침 수립) 공공기관의 장은 영상정보처리기기 운영·관리 방침을 마련하여 공개하여야 함

○ 공공기관은 영상정보처리기기 운영·관리 방침을 수립하고 이를 해당 기관의 인터넷 홈페이지에 게재하여 정보주체에게 공개하여야 합니다. (법 제25조제7항, 시행령 제25조 및 제31조제2항·제3항)

※ 홈페이지가 없는 경우 관보 또는 해당 공공기관 소재지에서 시·도 이상의 지역을 주된 보급지역으로 하는 일반일간신문, 일반주간신문 등에 게재 가능

※ 영상정보처리기기 운영·관리 방침 수립 대신에 영상정보처리기기 설치·운영에 관한 사항을 개인정보 처리방침에 포함하여 공개하는 것도 가능

방침에 포함하여야 할 사항

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

※ [별첨 1] 영상정보처리기기 운영·관리 방침 예시

7. (관리책임자 지정) 각급기관에서 개인영상정보의 처리에 관한 업무를 총괄하여 책임질 개인영상정보 관리책임자를 지정하여야 함

○ 개인영상정보 관리책임자는 각 기관 자체적으로 지정하여 관리하는 것을 원칙으로 합니다.(표준지침 제41조제1항)

관리책임자의 업무

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

○ 이미 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인정보 보호책임자가 개인영상정보 관리책임자의 업무를 수행할 수 있습니다. (표준지침 제41조제3항)

8. (영상정보의 목적 외 이용 및 제3자 제공) 공공기관은 법률에서 정하는 등 특별한 경우를 제외하고 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공할 수 없음

○ 공공기관은 원칙적으로 수집 목적을 넘어서 개인영상정보를 이용하거나 제3자에게 제공할 수 없으며, 다음의 예외사유에 해당하는 경우에 한하여 목적 외 이용·제공이 가능합니다.(법 제18조제1항·제2항)

【Q】 당초 범죄예방 목적으로 설치한 CCTV 영상자료를 민원인의 방문 여부를 확인하기 위해 열람하거나 제공할 수 있는지?

A. 원칙적으로 수집 목적을 넘어서 영상정보를 이용하거나 제3자에게 제공할 수 없으며, 정보주체의 동의, 다른 법률의 특별한 규정 등 예외 사유에 해당하는 경우에 한하여 이용 또는 제공할 수 있습니다.

개인영상정보 목적 외 이용·제3자 제공 제한의 예외

1. 정보주체의 별도의 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

※ 단, 5 ~ 9호는 공공기관의 목적 외 이용·제공 시에만 적용

【Q】경찰이나 검찰에서 수사목적으로 CCTV 자료를 요청했는데, 본인 동의 없이 제공해도 되는지?

A. 범죄수사와 공소제기 유지를 위해 수사기관에서 요청하는 경우 법 제18조제2항제7호 및 표준지침 제44조제1항제7호에 따라 본인 동의 없이 제공할 수 있습니다.

이 경우 본인 동의 없이 CCTV를 제공한다고 하더라도 수사에 필요한 최소한의 범위에서 제한적으로 제공하여야 하며, 요청기관에서도 관련 법령 및 요청 목적 등을 명확히 하고 최소한의 범위 내에서 자료제공을 요청하여야 합니다.

【Q】통계작성 및 학술연구 목적으로 영상정보를 요청하는 경우, 본인 동의 없이 제공해도 되는지?

A. 법 제18조제2항제4호에 따라 특정 개인을 알아볼 수 없도록 모자이크, 마스킹 처리 등 비식별화 조치 후 제공하는 것은 가능합니다.

【Q】 쓰레기를 무단투기 한 자의 신원 등을 확인하기 위한 목적으로 CCTV 영상을 공개하는 것이 가능한지?

A. 지방자치단체는「폐기물관리법」제8조 및 제68조에 따라 쓰레기 무단투기를 단속할 의무가 있습니다. 다만, 불특정 다수에게 무단투기자의 CCTV 영상을 공개하는 것은 법 제15조제1항제2호 및 제17조제1항제2호에 따른 법령상 의무를 준수하기 위한 '불가피한' 경우에 해당된다고 볼 수 없습니다.

다만, 법 제17조제1항제2호에 따라 공공기관이 법령 등에서 정하는 소관업무 수행을 위하여 불가피하게 수집한 개인정보는 당초 수집 목적 내에서 제3자에게 제공할 수 있는 바, 무단투기자의 CCTV 영상을 공개하여서는 아니되나 신원 확인을 위해 인근 주민 등 제한된 범위 내의 자에게 영상의 일부를 확인시키고 인적사항을 묻는 것은 가능합니다.

○ 개인영상정보를 제공받고자 하는 기관은 명칭/취급자, 목적/사유, 근거, 기간(파기예정일자 포함), 제공형태를 모두 기재한 문서(전자문서 포함)로 신청하여야 합니다.(표준지침 제9조)

※ 제공목적 달성을 위한 최소한의 기간으로 파기예정일자를 산정하기 곤란한 경우에는 30일 이내로 함

1. 요청기관의 명칭 및 요청 일자
2. 요청의 법적 근거
 -「개인정보 보호법」 제18조제2항제2호 및「민사집행법」제74조 등
3. 이용 목적 및 이용 기간
4. 파기 일시 및 파기 방법
 - 다른 법령에 따라 보관해야 하는 경우에는 그 근거를 명시
5. 요청하는 개인영상정보의 내용 ※ 예) 영상촬영일시, ○○장면
6. 요청하는 개인영상정보의 형태 ※ 예) 전자파일, 영상출력물 등
7. 제공 요청 방법 ※ 예) 이메일, 저장매체(USB 등)를 통한 직접(또는 우편)제공, 영상출력물의 직접(또는 우편)제공 등
8. 해당 업무 책임자 성명 및 연락처

○ 개인영상정보를 수집 목적 외로 이용하거나 제3자에게 제공하는 경우에는 다음의 사항을 기록하고 관리하여야 하며, 파기 등 개인영상정보의 안전성 확보를 위하여 필요한 조치를 하도록 요청하여야 합니다. (법 제18조제5항, 시행령 제15조, 표준지침 제46조제1항)

1. 개인영상정보 파일의 명칭 및 생성기간(녹화된 기간)
2. 이용하거나 제공받은 공공기관의 명칭 및 취급자(소속/직급/성명/연락처)
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간(제공의 경우 파기예정일자를 반드시 포함)
6. 이용 또는 제공의 형태
7. 제공한 이후 파기 여부 등 그 결과와 처리일자
8. 안전성 확보를 위하여 필요한 조치를 요청한 경우 그 내용 및 결과

※ [별첨 2] 개인영상정보 관리대장 활용 예시

○ 개인영상정보를 목적 외의 용도로 제공하는 기관은 제공사실을 관보 또는 홈페이지에 공개하여야 합니다.(법 제18조제4항, 시행규칙 제2조)

※ 제공한 날로부터 30일 이내에 “제공한 날짜・법적 근거・목적・개인정보의 항목”을 관보 게재 또는 홈페이지에 10일 이상 계속 게재함

○ 개인영상정보를 제공받은 기관은 개인영상정보의 안전성 확보를 위하여 필요한 조치와 안전한 관리를 위해 노력하여야 하며, 보유기간 만료, 목적 달성 등의 경우 제공받은 개인영상정보를 지체 없이 파기하고 그 결과와 처리일자를 제공한 기관에 통보하여야 합니다. 또한, 파기 예정일자가 도래할 경우 파기기간 연장을 문서(전자문서 포함)로 다시 요청하여야 합니다.

※ 다른 법령의 특별한 규정에 따라 사건기록 등 기록물에 포함하여 보존하여야 하는 경우에는 그 내용을 회신

※ 건별 통보가 곤란할 경우 제공하는 기관과 사전에 협의하여 분기 이내의 단위 기간을 정해 일괄적으로 회신할 수 있음

○ 개인영상정보를 제공한 기관은 제공이후 파기 등 결과 회신 여부를

분기 이내 단위 기간을 정하여 정기적으로 점검하여야 하며, 제공받은 기관이 파기 등 결과와 처리일자를 회신하여 오면 이를 개인영상정보 관리대장에 기록하고 관리하여야 합니다.

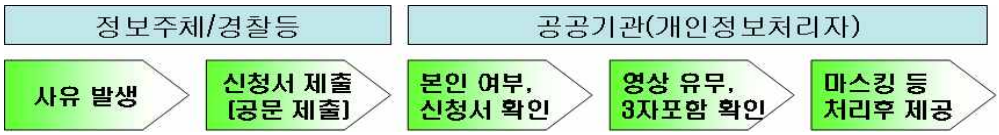
※ 미회신이 있는 경우 회신을 독려하고 필요한 관련 조치를 취하여야 함

개인영상정보 제공 시 준수사항 및 절차

□ **준수사항**

- 문서(전자문서 포함)로 명확한 목적 명시와 필요한 최소한의 자료 요청 및 제공
- 제공받은 자는 제공받은 목적 범위 내에서 이용과 안전한 관리
- 제공한 기관은 제공 사실에 대해 인터넷 등 공개 및 기록·관리
- 목적 달성 등 불필요하게 된 경우, 즉시 파기 및 파기사실 통보

□ **요청·제공 절차**



- (신 청) 정보주체 또는 수사관서에서 신청서 또는 공문으로 요청
- (접수·확인) 본인 여부, 신청서 내용 확인 및 해당 영상 유무 파악
- (내용 검토) 제3자 영상 포함 및 타인의 사생활 침해 등 검토
- (열람·제공) 영상화면의 현장 열람 또는 영상파일/출력물 등 제공, 필요시 제3자의 영상 모자이크 또는 마스킹 처리후 제공
- (안전 관리) 제공받은 자는 제공받은 목적 범위 내 이용 및 안전한 관리
- (파 기) 제공받은 자는 제공목적 달성한 후 즉시 파기 및 통보

9. (보관 및 파기) 영상정보처리기기에 의하여 수집된 영상정보는 보유기간이 만료된 후 지체 없이 삭제하여야 함. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러지 않음

○ 보유기간이 경과하면 개인영상정보를 지체 없이 파기해야 하며 '지체 없이' 란 보유기간 종료일로부터 5일 이내를 의미합니다.(표준지침 제11조제1항)

○ 해당기관의 특성에 따라 보유목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보유기간을 영상정보의 수집 후 30일 이내로 합니다. (표준지침 제45조제2항)

【Q】 영상정보의 보관기간은 반드시 30일 이내로 정해야 하는지?

A. 반드시 30일 이내로 하여야 하는 것은 아닙니다. CCTV 설치 목적 등 해당기관의 특성에 따라 보관 목적 달성을 위해 필요한 최소한의 기간이 30일을 초과하는 경우에는 이를 CCTV 운영·관리 방침에 반영하고 그 기간 동안 보관할 수 있습니다. 또한 다른 법령에 보관기간이 정해져 있는 경우에는 그에 따라야 합니다.

○ 공공기관이 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 합니다.(표준지침 제46조제2항)

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기일시(사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 대한 확인 시기)
3. 개인영상정보 파기 담당자

※ 표준지침 별지 서식 제3호 개인영상정보 관리대장 활용 가능

○ 영상정보의 파기시 출력물과 전자형태 등 존재 형태에 따라 복구 또는 재생이 불가능한 방법으로 파기해야 합니다.(법 제21조제2항)

○ 다른 법령에 따라 파기하지 아니하고 보존해야 하는 영상정보는 다른 영상정보와 분리하여 저장·관리해야 합니다.(법 제21조제3항)

10. (영상정보처리기기 설치·운영 사무의 위탁) 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 문서로 하여야 함

○ 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 다음의 내용이 포함된 문서로 하여야 합니다.(법 제26조제1항, 시행령 제26조제1항)

1. 위탁업무 수행 목적외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁하는 사무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 영상정보의 관리 현황 점검에 관한 사항
7. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

○ 업무를 위탁한 공공기관은 인터넷 홈페이지에 수탁자와 위탁하는 업무의 내용을 지속적으로 게재하여야 합니다. 다만, 인터넷 홈페이지에 공개가 불가능한 경우에는 다음 어느 하나의 방법으로 공개해야 합니다.(법 제26조제2항, 시행령 제28조제2항·제3항)

1. 위탁자의 사업장 등의 보기 쉬운 장소에 게시
2. 일반일간신문, 일반주간신문 또는 인터넷신문에 게재
3. 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 게재
4. 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급

○ 또한, 업무를 위탁한 공공기관은 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인영상정보를 안전하게 처리하는지를 감독하여야 하며, 수탁자는 위탁 받은 업무 범위를 초과하여 개인영상정보를 이용하거나 제3자에게 제공을 하여서는 아니 됩니다.(법 제26조제4항·제5항)

11. (열람등의 청구) 공공기관의 장은 정보주체에게 영상정보의 존재확인 및 열람·삭제를 요청받은 경우 지체 없이 필요한 조치를 취해야 함

○ 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인을 해당 영상정보처리기기운영자에게 요구할 수 있습니다.(법 제35조제1항, 표준지침 제48조제1항)

○ 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한합니다.(법 제35조제1항 및 제18조제2항)

○ 정보주체는 해당 공공기관의 장에게 개인영상정보에 대하여 열람 또는 존재확인을 요구할 수 있으며, 공공기관의 장은 이에 대하여 지체 없이 필요한 조치를 취하여야 합니다.(법 제35조제1항·제3항)

※ 공공기관의 경우 정보주체는 개인영상정보 열람·존재확인 청구서(표준지침 별지 서식 제2호)를 작성하여 청구하여야 함

○ 공공기관의 장은 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 합니다. (표준지침 제48조제3항)

○ 다만, 정보주체의 개인영상정보 열람등 요구가 다음 각 호의 사항에 해당하는 경우 요구를 거부할 수 있습니다. 이때에는 거부사유를 10일 이내에 서면으로 정보주체에게 통지하여야 합니다.(법 제35조제5항, 시행령 제42조제2항)

개인영상정보 열람등의 청구를 거부할 수 있는 사유

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우
2. 개인영상정보의 보관기간이 경과하여 파기한 경우
3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우(ex. 개인영상정보 열람으로 인하여 다른 사람의 사생활이나 정당한 이익을 침해할 우려가 큰 경우)

○ 열람등 조치를 취하는 때에는 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해 우려가 있는 경우 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취해야 합니다.(법 제35조제4항, 시행령 제42조제1항, 표준지침 제50조)

【Q】 본인이 영상자료 열람을 요청하는데 다른 사람이 함께 찍힌 경우에는 어떻게야 하나?

A. 영상자료에 다른 사람이 함께 찍힌 경우 원칙적으로 다른 사람은 식별할 수 없도록 모자이크 처리 등을 해서 최소한으로 제공하여야 합니다.

【Q】 민원인이 지갑을 두고 가서, 이를 가져간 사람의 확인을 위해 CCTV 자료 열람을 요청한 경우 열람이 가능한지?

A. 정보주체는 자신의 영상정보가 아니더라도 해당 영상정보주체의 주소불명 등으로 동의 얻을 수 없는 경우이면서 정보주체의 급박한 생명, 신체, 재산상 이익을 위하여 필요한 경우에 한해서 타인에 관한 영상자료를 열람할 수 있습니다.

다만, 그 범위는 필요 최소한도로 제한되며, 영상정보처리기기운영자나 개인정보처리자가 관련 영상을 먼저 확인 후 해당 부분에 대해서만 열람시켜주는 것이 바람직합니다.

※ 이 경우 영상정보처리기기의 특성상 일정기간이 지나면 영상자료가 삭제된다는 점에서 CCTV영상자료는 그 자체로 급박성이 있다고 봄.

○ 공공기관은 정보주체가 개인영상정보에 대한 열람등 요구를 한 경우 그에 대한 조치사항과 내용을 기록·관리하여야 합니다.(표준지침 제48조제5항 및 제49조)

정보주체의 개인영상정보 열람 등 요구 시 기록사항

1. 개인영상정보 열람 등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람 등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람 등의 목적
4. 개인영상정보 열람 등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

※ 표준지침 별지 서식 제3호 개인영상정보 관리대장 활용 가능

12. (개인영상정보의 안전성 확보를 위한 조치) 공공기관의 장은 개인영상정보가 분실·도난 ·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 함

○ 공공기관의 장은 영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 취하여야 합니다.(법 제29조, 시행령 제30조제1항, 표준지침 제51조)

○ 공공기관의 장은 영상정보처리기기에 의하여 수집·처리되는 영상정보로의 접근권한을 총괄책임자 및 운영책임자 등 지정된 최소한의 인원으로 제한하여야 합니다.

개인영상정보에 대한 안전성 확보조치

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
   ① 개인영상정보 관리책임자 지정
   ② 개인영상정보 관리책임자 및 취급자의 역할 및 책임에 관한 사항
   ③ 안전성 확보조치에 관한 사항
   ④ 개인영상정보 취급자 교육
   ⑤ 그 밖에 개인영상정보의 안전성 확보에 필요한 조치에 관한 사항
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용
   (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치,
   개인영상정보파일에 대한 비밀번호 설정 등)
   ※ 괄호안의 내용은 안전한 저장 전송 방법의 예시를 든 것이며,
   상황에 맞게 적절한 안전조치 기술을 적용하시면 됩니다.
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

※ 비공개 장소에 설치된 영상정보처리기기에 대한 안전성 확보조치는 공개된 장소에 대한 영상정보처리기기에 관한 규정을 준용하는 것이 바람직합니다.

○ 공공기관의 장은 영상정보처리기기에 접근 권한이 없는 자가 영상정보처리기기를 함부로 조작하거나 모니터링 할 경우 관련 법령에 따라 처벌받을 수 있다는 사실의 안내판을 모니터링 화면 옆이나 영상정보처리기기 관리 본체에 부착하여 접근 권한 없는 자의 임의적 접근 및 조작 등을 방지하는 것이 바람직합니다.

13. (개인영상정보처리기기의 설치·운영에 대한 점검) 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우 표준개인정보지침 준수 여부에 대한 자체점검을 한 후 관련 내용을 행정자치부장관에게 통보해야 함

○ 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 표준 개인정보보호지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 행정자치부장관에게 통보하고, 개인정보보호 종합지원시스템(http://intra.privacy.go.kr)에 등록하여야 합니다.(표준지침 제52조제1항)

※ 매년 자체점검 결과를 다음 해 3월 31일까지 등록(시스템 등록으로 통보 갈음함)

자체 점검 시 고려사항

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

○ 공공기관의 장은 제1항과 3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 합니다.(표준지침 제52조제2항)

[**별첨 1**] 영상정보처리기기 운영・관리 방침 예시

【 영상정보처리기기 운영·관리 방침 】

본 _____(이하 본 기관이라 함)는 영상정보처리기기 운영·관리 방침을 통해 본 기관에서 처리하는 영상정보가 어떠한 용도와 방식으로 이용 관리되고 있는지 알려드립니다.

1. 영상정보처리기기의 설치 근거 및 설치 목적

본 기관은「개인정보 보호법」제25조 제1항에 따라 다음과 같은 목적으로 영상정보처리기기를 설치·운영 합니다.

- 시설안전 및 화재 예방
- 고객의 안전을 위한 범죄 예방

(주차장에 설치하는 경우)

- 차량도난 및 파손방지

※ 주차대수 30대를 초과하는 규모의 경우 「주차장법 시행규칙」제6조제1항을 근거로 설치·운영 가능

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
00대	건물로비, 주차장 입구

3. 관리책임자 및 접근권한자

귀하의 영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자를 두고 있습니다.

	이름	직위	소속	연락처
관리책임자	홍길동		0000과	00-0000-0000
접근권한자				

4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	촬영일로부터 30일	000실 (보관시설 명)

- 처리방법 : 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제(출력물의 경우 파쇄 또는 소각)합니다.

5. 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 (해당하는 경우만)

본 기관은 아래와 같이 영상정보처리기기 설치 및 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

수탁업체	담당자	연락처
OO시스템	홍길동	02) 000-0000

6. 개인영상정보의 확인 방법 및 장소에 관한 사항

- 확인 방법 : 영상정보 관리책임자에게 미리 연락하고 본 기관을 방문하시면 확인 가능합니다.
- 확인 장소 : OO부서 OO팀

7. 정보주체의 영상정보 열람 등 요구에 대한 조치

귀하는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 영상정보처리기기 운영자에게 요구하실 수 있습니다. 단, 귀하가 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한정됩니다.

본 기관은 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체 없이 필요한 조치를 하겠습니다.

8. 영상정보의 안전성 확보조치

본 기관에서 처리하는 영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본 기관은 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등부여하고 있고, 개인영상정보의 위·변조 방지를 위하여 개인영상정보의 생성 일시, 열람 시 열람 목적·열람자·열람 일시 등을 기록하여 관리하고 있습니다. 이 외에도 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

9. 개인정보 처리방침 변경에 관한 사항

이 영상정보처리기기 운영·관리방침은 2012년 O월 OO일에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 시행하기 최소 7일전에 본 기관 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 공고일자 : 2012년 O월 OO일 / 시행일자 : 2012년 O월 OO일

[별첨 2] 개인영상정보 관리대상 활용 예시

【 개인영상정보 관리대장 】

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간 및 파기예정일자	파기 등 결과 및 처리일자	안전관리 요청 및 결과
1	□ 이용 □ 제공 □ 열람 □ 파기										
2	□ 이용 □ 제공 □ 열람 □ 파기										
3	□ 이용 □ 제공 □ 열람 □ 파기										
4	□ 이용 □ 제공 □ 열람 □ 파기										
5	□ 이용 □ 제공 □ 열람 □ 파기										
6	□ 이용 □ 제공 □ 열람 □ 파기										
7	□ 이용 □ 제공 □ 열람 □ 파기										

<참고>

개인영상정보 관리대장 작성요령

o 구분 : 이용/제공/열람/파기 중 1개에 √ 표시
  - 이용 : 개인정보처리자가 영상자료 관리 등을 위해 이용하는 경우
  - 제공 : 개인정보처리자 및 정보주체가 아닌 제3자에게 주는 경우
    (제3자가 방문하여 현장에서 화면을 확인한 경우에도 제공에 해당)
  - 열람 : 정보주체에게 본인의 영상자료를 주는 경우
    (정보주체에게 출력물 등 영상자료를 교부하는 경우에도 열람에 해당)
  - 파기 : 이용·제공·열람 후 파기한 경우 파기 내용을 기재(자동 삭제 포함)

o 일시 : 신청받은 일시 기재('12.10.10. 14:00 등)

o 파일명/형태 : 관리하고 있는 파일 명칭과 파일형태를 기재('12.10.5일 3～10번 CCTV/동영상, 121005-0003-00동.mp4 등)

o 담당자 : 제공기관의 업무처리 담당자 소속/직급/성명 기재(00과 00직급 홍길동)

o 목적/사유 : 신청기관이 제시한 목적/사유를 구체적으로 기재(청소년 범죄수사, 가출자녀 경로확인, 자전거 도난확인 등)

o 이용·제공받는 제3자/열람 등 요구자 : 책임 소재 명확화 및 사후 관리를 위해 신청기관 명칭과 취급자의 소속, 직급, 성명, 연락처 등을 기재(00경찰서 00계 직급 박길동 02-123-4567)

o 이용·제공하는 근거 : 법령상 이용 또는 제공근거가 있는 경우 법령의 명칭과 조항을 기재
  - 근거 법령이 없을 경우 신청 문서의 제목과 문서번호 등을 기재

o 이용·제공 형태 : 자료열람, 자료복제(프린트, F/D, CD, USB), 기타(000형태)로 구분하여 기재

o 기간 및 파기예정일자 : 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간을 기재('12.10.11～11.10)
  - 제공의 경우에는 파기예정일자를 반드시 기재(파기예정 '12.11.10)
  - 사전에 파기 시기를 정하여 자동 삭제하는 경우에는 파기 주기 및 자동 삭제 여부에 대한 확인 시기를 기재(30일 주기 자동 파기, 매월 1일 확인)

o 파기 등 결과 및 처리일자
  - 결과 회신 : 통보받음(수사종결 파기, '12.10.10, 파기자 김길동), 통보받음(기록물 보존, '12.10.10), 통보받음(검찰 등 타기관 이첩, '12.10.10)
  - 자료 반환 : 자료반환('12.10.11) 받은 후 파기함(12.10.11, 파기자 이길동)
  - 기타 : 개인 등에게 타인의 얼굴을 모두 가리고 열람·제공하여 파기 결과 확인이 불필요한 경우에는 "타인영상 제거 후 제공('12.10.10)" 등으로 기재
  - 파기기간 연장 : 연장 내용을 우선 기재하고, 향후 회신 등 결과를 추가 기재

o 안전관리 요청 및 결과 : 영상자료를 제공할 때 안전한 관리에 대하여 따로 요청한 내용이 있는 경우에는 그 내용과 결과를 기재

개인정보보호
자율점검 가이드라인
[개인정보처리자용]

2015년 6월

행 정 자 치 부
개 인 정 보 보 호 과

머리말

1. 본 자율점검 가이드라인은 “개인정보보호법*”에 따라 자율점검을 수행하는 개인정보처리자용으로 작성되었습니다.

*개인정보보호법 법률 제12844호(시행 2014.11.19.), 행정자치부고시 제2014-7호(시행 2014. 12. 30.)를 기준으로 작성

2. 자율점검표의 항목 선정 기준은 다음과 같습니다.

   1) 벌칙 및 과태료(제71조, 제72조, 제73조, 제75조)가 있는 조항을 기준으로 선정

   2) 상기 기준으로 선정된 항목 중 제19조, 제20조, 제25조, 제34조, 제35조, 제36조, 제37조, 제59조, 제60조, 제63조, 제64조, 기타 유출과 관련된 조항은 제외

3. 본 자율점검 가이드라인과 개인정보보호법 현장검사 및 행정처분은 무관하며, 세부적인 벌칙·과태료는 개인정보보호법을 참고하십시오.

4. 본 문서를 자율점검 외의 목적으로 사용하는 것을 금지하며, 부득이하게 사용할 경우 반드시 출처를 고지해주시기 바랍니다.

목 차

Ⅰ 자율점검표 작성 개요 ····· 1

1 용어의 정의 ····· 1

2 자율점검표 작성법 ····· 3

Ⅱ 세부항목별 점검 방법 및 평가 기준 ····· 5

1 개인정보의 수집·이용 동의(법 제15조) ····· 5

2 최소 수집 및 서비스 제공 거부(법 제16조) ····· 7

3 개인정보의 제공(법 제17조) ····· 8

4 개인정보의 이용·제공 제한(법 제18조) ····· 10

5 개인정보의 파기(법 제21조) ····· 13

6 동의를 받는 방법(법 제22조) ····· 14

7 민감정보의 처리 제한(법 제23조) ····· 17

8 고유식별정보의 처리 제한(법 제24조) ····· 18

9 주민등록번호의 처리 제한(법 제24조의2) ····· 19

10 업무위탁에 따른 처리 제한(법 제26조) ····· 20

11 안전조치의무(법 제29조) ····· 22

12 개인정보 처리방침의 수립·공개(법 제30조) ····· 37

13 개인정보 보호책임자의 지정(법 제31조) ····· 38

[붙임1] 네트워크 전송 구간 암호화 여부 검사 방법(wireshark 사용법) ····· 39

Ⅰ 자율점검표 작성 개요

1 용어의 정의

다음 용어에 대한 정의는 개인정보보호법, 행정자치부고시 제2014-7호 (안전성확보조치기준)를 참조하였습니다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

7. "소상공인"이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」제2조에 해당하는 자를 말한다.

8. "중소사업자"란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」제2조제1항제1호에 따른 광업·제조업·건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.

9. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.

10. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

11. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

12. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

13. "내부관리계획"이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준을 말한다.

14. "비밀번호"라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

15. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

16. "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

17. "보조저장매체"라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.

18. "위험도 분석"이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.

19. "모바일 기기"라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

20. "공개된 무선망"이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

2 자율점검표 작성법

[자 율 점 검 개 요]

1. 개인정보 처리 업무 및 업무담당자 파악

▼

2. 개인정보 현황(개인정보파일, 개인정보처리시스템) 파악

▼

3. 자율점검표 작성

1. 개인정보 업무 및 업무담당자 파악

❍ 개인정보 자율점검표 작성에 앞서, 개인정보처리자가 처리하는 개인정보와 관련된 모든 업무 및 업무 담당자(개인정보취급자)를 파악

▶ 개인정보 수집 여부는 해당 업무 담당자가 가장 잘 알고 있기 때문에, '2. 개인정보 현황' 파악에 앞서 업무 담당자를 찾아야함

2. 개인정보 현황 파악

❍ 앞서 파악한 업무 담당자를 통해 개인정보파일, 개인정보처리시스템 현황을 파악하여 엑셀파일 '2.현황' 시트를 작성

- (개인정보파일현황파악) 개인정보처리자는 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 개인정보파일로 간주하여 현황을 파악

▶ 개인정보보호법제15조제1항에 따라 수집 출처 및 수집 경로가 다를 경우 다른 개인정보파일로 분류하고, 기존 개인정보파일에서 파생되는 개인정보파일의 경우 원래의 개인정보파일로 간주하여 처리함

Q) 개인정보처리자는 1개의 홈페이지를 보유중이고 해당 홈페이지에서 회원가입을 받고 비회원게시판(이름, 이메일주소 수집)을 운영한다. 이 경우 개인정보처리자는 몇 개의 개인정보파일을 처리하는가?

A) 개인정보처리자는 총 2개의 개인정보파일을 처리함(홈페이지 회원정보의 경우 홈페이지 회원가입을 통해 개인정보를 수집하고, 비회원 게시판의 경우 게시글 입력 시 개인정보를 수집하기 때문에 이 경우 수집되는 경로가 다른 경우에 해당)

- (개인정보처리시스템현황파악) 개인정보처리자는 파악된 개인정보파일이 전자적인 데이터베이스 시스템(DBMS)으로 처리될 경우, 개인정보처리시스템으로 간주하여 현황을 파악

3. 자율점검 표(엑셀) 작성

❍ 개인정보파일별로 작성하는 것이 원칙임

❍ 다만, 일부 항목의 경우 개인정보처리자*, 개인정보처리시스템**별로 작성함(세부내용은 엑셀 '1.항목표' 작성단위 칼럼 참조)

* 제26조, 제29조(내부관리계획, 물리적접근통제), 제30조, 제31조

** 제29조(접근권한, 암호화, 접속기록, 보안프로그램)

II 세부항목별 점검 방법 및 평가 기준

1 개인정보의 수집·이용 동의(법 제15조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제15조(개인정보의 수집·이용 동의)	1-1. 개인정보 수집·이용 근거			
	1-2. 정보주체 동의 시 필수 고지항목(4개*) 고지 여부			
	1-3. 필수 고지항목(4개*) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

1-1. 개인정보 수집·이용 근거

❍ 개인정보 수집·이용 근거에 따라 정보주체로부터 개인정보를 수집하는지 확인

※ 다음 '개인정보 수집·이용 근거'를 참조하여 ①~⑥ 중 해당하는 숫자를 양호에 체크 단, ①~⑥에 해당하지 않고 개인정보를 수집할 경우 개선필요에 체크

< 개인정보 수집·이용 근거 >

① 정보주체의 동의를 받은 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
④ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
⑥ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

1-2. 정보주체 동의 시 필수 고지항목(4개) 고지 여부

※ 앞의 '1. 개인정보 수집·이용 근거 항목'에서 ①을 선택하지 않았을 경우 "해당없음"에 체크

❍ 정보주체의 동의를 받고 개인정보를 수집·이용하는 경우 필수 고지항목 4개를 고지하고 동의 받는지를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보의 수집·이용 목적
② 수집하려는 개인정보의 항목
③ 개인정보의 보유 및 이용 기간
④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

☞ **정보통신망법에 따라 ①~③번은 고지하나, 상당수 홈페이지에서 ④를 고지하지 않고 있음, 또한 개인정보처리방침 전체를 고지하면서 ④가 포함되지 않은 상태로 고지하는 사례 다수 있음**

1-3. 필수 고지항목(4개) 내용의 적정 여부

※ 앞의 '1. 개인정보 수집·이용 근거 항목'에서 ①을 선택하지 않았을 경우 "해당없음"에 체크

❍ 정보주체의 동의를 받고 개인정보를 수집·이용하는 경우 필수 고지항목(4개)의 내용이 적정한지 확인

- 개인정보의 수집·이용 목적이 적정한지 여부 확인
- 수집하려는 개인정보의 항목과 보유 및 이용기간 설정이 수집 목적 달성을 위해 적합하게 설정되었는지 여부 확인
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

※ 필수항목, 선택항목에 따른 수집 목적을 명확히 하고, 목적 달성을 위해 불필요한 수집항목과 보유기간 등은 수집·이용하는 목적에 맞게 조정 필요

☞ **'수집하려는 개인정보 항목'에서 성명이라고 고지하고 회원정보 입력 시 이름을 수집하는 경우(유사한 내용이라도 고지 시 명칭과 수집 시 명칭이 일치해야 함)**

☞ **'보유 및 이용 기간' 고지 시 구체적 보유기간을 명시하지 않고 "이용목적 달성 시 까지 보관"이라고 고지하는 경우**

2 최소 수집 및 서비스 제공 거부(법 제16조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제16조(최소 수집 및 서비스 제공 거부)	2-1. 목적에 필요한 최소한의 개인정보 수집 여부			
	2-2. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부			

□ 점검 방법 및 평가 기준

2-1. 목적에 필요한 최소한의 개인정보 수집 여부

❍ 정보주체로부터 수집하는 필수정보가 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보인지 여부 확인

※ 최소한의 개인정보 수집 여부에 대한 입증 책임은 개인정보처리자가 부담

2-2. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부

❍ 정보주체의 동의 획득 시 최소한의 정보(필수정보) 외의 개인정보 수집에 동의하지 않는다는 이유로 회원 가입 또는 기본적인 서비스 제공이 불가능한지 여부 확인

※ 동의하지 않는다는 이유로 회원 가입 또는 서비스 제공이 불가능할 경우, 개선필요에 체크

- 특히, 홈페이지 회원 가입 시 필수정보가 아닌, 선택정보로 되어 있는 개인정보를 입력하지 않을 경우 회원가입이 불가능한지 확인

☞ **홈페이지에서 선택 사항에 대한 동의 체크를 하지 않으면 다음으로 넘어가지 않은 사례 있음**

3 개인정보의 제공(법 제17조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제17조(개인정보의 제공)	3-1. 개인정보 제3자 제공 근거			
	3-2. 정보주체 동의 시 필수 고지항목(5개*) 고지 여부			
	3-3. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

3-1. 개인정보 제3자 제공 근거

❍ 개인정보 제공 근거에 따라 정보주체의 개인정보를 제3자에게 제공하는지 여부를 확인

※ 다음 '개인정보 제공 근거'를 참조하여 ①~④ 중 하나의 숫자를 양호에 체크
만일, ①~④에 해당하지 않고 개인정보를 제공할 경우 개선필요에 체크

※ 고유식별정보, 민감정보의 경우 법령 상 제공하여 처리할 수 있는 규정이 있는 경우 동의 없이 제공 가능하며, 그렇지 않은 경우에는 동의 받고 제공할 수 있음
다만, 고유식별정보 중 주민등록번호는 법령 규정 외에는 처리 할 수 없음

< 개인정보 제공 근거 >

① 정보주체의 동의를 받은 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
④ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

3-2. 정보주체 동의 시 필수 고지항목(5개) 고지 여부

※ 앞의 '3-1. 개인정보 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크

❍ 정보주체의 동의를 통해 개인정보를 제3자에게 제공하는 경우 필수 고지항목(5개)을 고지하고 동의를 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

☞ **홈페이지에서 제공 동의 획득 시 ⑤번에 대한 고지 없이 동의 받는 사례 있음**

3-3. 필수 고지항목(5개) 내용의 적정 여부

※ 앞의 '3-1. 개인정보 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크

❍ 온라인 회원 가입 서식과 홈페이지 게시판, 기타 서식을 통해 개인정보 제3자 제공의 동의 획득 시 고지항목(5개)의 적정 여부를 확인

- 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
- 제공받는 자의 개인정보 이용목적이 적정한지 여부 확인
- 제공하려는 개인정보의 항목과 제공받는 자의 보유 및 이용기간 설정이 이용 목적 달성을 위해 불가피하게 설정되었는지 여부
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

※ 법령 상 규정 또는 의무 이행을 위해 제공하는 경우 동의 획득하지 않고 제공할 수 있음, 다만, 법령에서 정한 목적 및 범위 내에서만 처리해야하며, 제공하는 사항에 대해 개인정보처리방침을 통해 공개해야 함

☞ **법령 상 정한 목적 및 범위를 초과하여 이용제공 하는 경우 처벌 받을 수 있음**

4 개인정보의 이용·제공 제한(법 제18조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제18조(개인정보의 이용·제공 제한)	4-1. 개인정보 목적 외 이용·제공 근거			
	4-2. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개*) 고지 여부			
	4-3. 필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

4-1. 개인정보 목적 외 이용·제공 근거

❍ 「개인정보 목적 외 이용 및 제3자 제공 근거」에 따라 정보주체의 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는지 확인

※ 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 다음 '개인정보 목적 외 이용 및 제3자 제공 근거'에 해당하는 경우 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있음. 다만, ⑤~⑨까지의 경우 공공기관의 경우로 한정함

※ 다음 '개인정보 목적 외 이용 및 제3자 제공 근거'를 참조하여 ①~⑨ 중 하나의 숫자를 양호에 체크
만일, ①~⑨에 해당하지 않고 개인정보를 목적 외 이용하거나 이를 제3자에게 제공할 경우 개선필요에 체크

< 개인정보 목적 외 이용 및 제3자 제공 근거 >

① 정보주체로부터 별도의 동의를 받은 경우
② 다른 법률에 특별한 규정이 있는 경우
③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
⑧ 법원의 재판업무 수행을 위하여 필요한 경우
⑨ 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

4-2. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개) 고지 여부

※ 앞의 '4-1. 개인정보 목적 외 이용 및 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크

❍ 정보주체의 동의에 의한 목적 외 이용 및 제3자 제공 시 필수 고지항목(5개)을 고지하고 동의 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

① 개인정보를 제공받는 자
② 개인정보의 이용목적(제공 시 제공받는 자의 개인정보 이용 목적)
③ 이용 또는 제공하는 개인정보의 항목
④ 개인정보의 보유 및 이용기간(제공 시 제공 받는 자의 보유 및 이용 기간)
⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

4-3. 필수 고지항목(5개) 내용의 적정 여부

※ 앞의 '4-1 개인정보 목적 외 이용 및 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 "해당없음"에 체크

❍ 정보주체의 동의에 의한 목적 외 이용 및 제3자 제공하는 경우 필수 고지항목(5개)의 내용이 적정한지

- 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
- 제공받는 자의 개인정보 이용 목적이 적정한지 여부 확인
- 제공하려는 개인정보의 항목과 제공받는 자의 보유 및 이용기간 설정이 이용 목적 달성을 위해 불가피하게 설정되었는지 여부
- 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인

5 개인정보의 파기(법 제21조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제21조(개인정보의 파기)	5-1. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부			
	5-2. 법령에 따라 보존할 경우 별도 분리 보관 여부			

□ 점검 방법 및 평가 기준

5-1. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부

❍ 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과된 경우에는 지체 없이(보유기간 종료일로부터 5일 이내) 파기하는지 여부 확인

- 다만, 법령에 따라 보존이 필요한 경우에는 법령에 명시된 기간 동안 보존 할 수 있음

※ 법령에 따라 보존 필요 시 기존 개인정보(파일)과 분리하여 보관하여야 함

☞ **수집 목적이 달성되고, 보유기간이 경과된 후에도 보관 중인 경우 사례 흔함**

5-2. 법령에 따라 보존할 경우 별도 분리 보관 여부

❍ 계약종료 및 탈퇴 등을 이유로 해당 정보주체의 개인정보를 삭제해야하나, 법령에 따라 보존이 필요한 경우 파기시점이 도래하지 않은 개인정보들과 분리(다른 table에 분리)하여 보관하는지 확인

- 접근권한은 필수 요원(소송 담당자 등)에게만 부여해야 함

☞ **법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것이며, 파기 시 삭제하지 않고 단순히 테이블 필드에 플래그 형태로 남기는 사례 있음**

☞ **법령에 따라 보존하여야 하는 경우로는 전자상거래 거래기록 등이 있음**

6 동의를 받는 방법(법 제22조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제22조(동의를 받는 방법)	6-1. 동의 사항의 구분 동의 여부			
	6-2. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부			
	6-3. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부			
	6-4. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부			
	6-5. 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부			

□ 점검 방법 및 평가 기준

6-1. 동의 사항의 구분 동의 여부

❍ 동의의 내용과 의미를 명확하게 인지한 상태에서 동의 여부를 결정할 수 있도록 통상의 동의*와 구분해서 동의 받고 있는지 여부 확인

*개인정보 수집·이용 동의(제15조 제1항 제1호)

< 구분 동의가 필요한 경우 >

① 제3자 제공 동의(제17조 제1항 제1호)
② 국외 제3자 제공 동의(제17조 제3항)
③ 목적 외 이용·제공 동의(제18조 제2항 제1호)
④ 마케팅 목적 처리 동의(제22조 제3항)
⑤ 법정대리인의 동의(제22조 제5항)
⑥ 민감정보의 처리 동의(제23조 제1항 제1호)
⑦ 고유식별정보 처리 동의(제24조 제1항 제1호)

☞ **위 7가지 동의 사항은 개인정보 수집에 따른 기본동의과 별도록 각각 구분하여 동의를 받아야 하는 사항이나, 일반동의만 1회 받는 사례 있음**

6-2. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부

❍ 정보주체의 동의가 필요 없는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하는지 확인

< 동의가 필요 없는 개인정보 >

① 계약의 체결 및 이행을 위해 필수적인 정보 ② 급박한 생명·신체·재산상 이익보호를 위해 필요한 정보 ③ 법령상 의무 준수를 위해 불가피한 정보 ④ 개인정보처리자의 정당한 이익을 위해 필요한 정보 등

- 고유식별정보 및 민감정보의 경우에는 계약의 체결 이행 등을 위해 필요하다고 해도 제24조, 제23조에 의거, 별도 동의 받거나 관련 법령에 의해 처리를 허용하고 있는지 여부 확인

- 개인정보처리자가 자신의 정당한 이익을 위해 동의 없이 처리한 경우 개인정보처리자가 이를 입증*할 수 있는지 확인

* 동의 없이 처리할 수 있는 개인정보라는 입증은 개인정보처리자가 해야하며, 입증하지 못하는 경우 동의 받지 않고 수집하는 것으로 처벌될 수 있음

※ 대부분 기관에서 동의 없이 수집 가능한 경우에도 추후 분쟁 등을 피하거나, 법령상 목적 외에 부가적인 목적 달성을 위해 필수사항에 포함하여 동의를 받고 있음

6-3. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부

❍ 재화나 서비스를 홍보하거나 판매를 권유하기 위한 동의 획득 시 일반적인 개인정보 동의 여부와 구분하고 있는지 확인

☞ **개인정보 수집 목적에 '신제품 소개 및 안내' 등 홍보 및 마케팅 관련 목적을 기술 하고도, 홍보 및 마케팅 동의를 별도로 구분하여 받지 않고, 일반동의만 받는 사례 있음**

6-4. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부

❍ 선택정보를 수집하거나, 홍보 권유를 위한 개인정보 동의에 대해 미동의 이유로 홈페이지 회원 가입 등 기본적인 재화 또는 서비스 제공을 거부하고 있는지 확인

< 기본적인 서비스 제공과 관계없는 동의 사항 >

① 선택정보의 처리에 대한 동의
② 직접 마케팅에 대한 동의
③ 목적외 이용·제공에 대한 동의

☞ **홈페이지에서 마케팅 목적 또는 선택정보 미동의시 회원가입이 안되는 사례 있음**

6-5. 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부

❍ 개인정보파일의 정보주체들 중 만 14세 미만의 아동이 있을 경우, 해당 아동으로부터 개인정보를 수집 시 법정대리인으로부터 동의를 받았는지 확인

☞ **개인정보처리자는 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있음**

7 민감정보의 처리 제한(법 제23조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제23조(민감정보의 처리 제한)	7-1. 민감정보 처리 근거			

□ 점검 방법 및 평가 기준

7-1. 민감정보 처리 근거

❍ 민감정보가 포함된 개인정보파일을 처리할 경우, 정보주체에게 별도 동의를 받거나 법령에 근거하였는지 확인

※ 정보주체의 동의에 의해 민감정보를 처리하는 경우 양호에 체크
법령의 특별한 규정에 따라 민감정보를 처리하는 경우 양호에 '㊊' 표시

< 민감정보의 구분 >

① 사상·신념에 관한 정보 ② 노동조합·정당의 가입·탈퇴에 관한 정보
③ 정치적 견해에 관한 정보 ④ 건강, 성생활에 관한 정보
⑤ 유전자 검사 결과로 얻어진 유전정보 ⑥ 범죄경력자료에 해당하는 정보

☞ **민감정보를 수집하면서 구분하여 동의 받지 않고 통상의 동의만 받는 사례 다수 있음**

8 고유식별정보의 처리 제한(법 제24조)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제24조(고유식별정보의 처리 제한)	8-1. 고유식별정보* 처리 근거 * 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호			

□ 점검 방법 및 평가 기준

8-1. 고유식별정보 처리 근거

❍ 고유식별정보(주민등록번호를 제외)가 포함된 개인정보파일을 처리할 경우, 정보주체에게 별도 동의를 받거나 법령에 근거하였는지 확인

※ 정보주체의 동의에 의해 고육식별정보를 처리하는 경우 양호에 체크
법령의 특별한 규정에 따라 고유식별정보를 처리하는 경우 양호에 '㊊' 표시

< 고유식별정보의 범위 >

① 주민등록번호* ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호

* '14.8.7일 이후 법령 상 처리가 허용된 경우만 처리 할 수 있으며, 보유하고 있는 정보는 '16.8.6일까지 파기

☞ **고유식별정보를 수집하면서 구분하여 동의받지 않고 통상의 동의만 받는 사례 다수 있음**

9 주민등록번호의 처리 제한(법 제24조의2)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제24조의2(주민등록 번호 처리의 제한)	9-1. 법에 근거하지 않은 주민등록번호 수집 및 처리 여부			
	9-2. 주민등록번호 외 회원가입 방법 제공 여부			

□ 점검 방법 및 평가 기준

9-1. 법에 근거하지 않은 주민등록번호 수집 및 처리 여부

❍ 법령에서 구체적으로 주민등록번호의 처리를 요구하거나, 허용한 경우에만 주민등록번호를 처리하고 있는지 여부 확인

※ 법령의 특별한 규정에 따라 주민등록번호를 처리하는 경우 양호에 체크

※ 법령 상 처리가 허용된 경우만 처리 할 수 있으며, 보유하고 있는 정보는 '16.8.6일까지 파기

9-2. 주민등록번호 외 회원가입 방법 제공 여부

❍ 공공기관 및 공공기관 외의 인터넷 홈페이지를 운영하는 자로 전년도말 기준 직전 3개월간 인터넷 홈페이지를 이용자 수가 하루 평균 1만명 이상인 경우

- 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(예: I-PIN, 공인인증서, 휴대전화 인증 등)을 제공하고 있는지 확인

10 업무위탁에 따른 처리 제한(법 제26조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제26조(업무위탁에 따른 처리 제한	10-1. 위탁 시 필수사항(7) 포함한 문서(계약서)에 의한 계약 여부 * 7개 : 목적외 처리금지, 기술·관리적 보호조치, 목적·범위, 재위탁 제한, 접근제한 등 안전조치, 관리·감독사항, 손해배상책임			
	10-2. 수탁자 공개 여부			

□ 점검 방법 및 평가 기준

10-1. 위탁 시 필수사항(7개) 포함한 문서(계약서)에 의한 계약 여부

❍ 개인정보 처리에 관한 업무를 수탁하는 경우 필수사항(7개)을 포함한 문서(계약서)에 의한 계약을 체결하는지 확인

- 보안 약정서, 협약서 등의 형태의 계약 부속서류라 하더라도 필수사항(7개)이 모두 포함되어 있는 경우에는 인정됨

< 위탁계약 시 문서에 포함될 필수사항 >

① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적·관리적 보호조치에 관한 사항
③ 위탁업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

☞ **계약서에 비밀 누설 금지 등의 사항만 포함하고, 필수사항(7개)을 누락한 사례 다수 있음**

10-2. 수탁자 공개 여부

❍ 개인정보의 처리 업무를 위탁하는 경우 수탁자를 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하고 있는지 여부 확인

- 인터넷 홈페이지에 공개할 수 없는 경우 다른 방법으로 공개 필요

< 인터넷 홈페이지가 없는 경우 수탁자 공개 방법 >

① 사업장의 보기 쉬운 장소에 게시
② 관보 또는 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
③ 정보주체에게 배포하는 각종 소식지에 포함하여 연 2회 이상 발행
④ 계약서 등에 실어 발급하는 방법

☞ **수탁사를 누락하거나, 업무 단위로 묶어 개별 수탁사를 파악하기 어려운 사례 있음**

11-1 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	1.내부관리계획 수립·시행	11-1-1. 내부관리계획 수립·시행 여부			
		11-1-2. 내부관리계획의 필수 반영사항(5개*) 포함 여부 * 5개 : 보호책임자 지정, 보호책임자/취급자의 역할·책임, 안전성 확보 조치, 취급자 교육, 수탁자에 대한 관리·감독			

□ 점검 방법 및 평가 기준

11-1-1. 내부관리계획 수립·시행 여부

❍ 개인정보의 안전한 처리를 위한 내부관리계획을 수립·시행하고 있는지 확인(단, 소상공인은 내부관리계획을 수립하지 아니할 수 있음)

- 내부관리계획이라는 명칭 이외의 다른 명칭(예: 개인정보보호정책 등)으로 수립하여도 점검항목 11-1-2의 사항이 모두 포함되어야 내부관리계획으로 인정됨

< 소상공인 및 상시근로자 정의 >

▸ 소상공인 : 「소기업 및 소상공인 지원을 위한 특별조치법」 제2조제2호에 의거 '광업·제조업·건설업 및 운수업'의 경우 상시근로자의 수가 10인 미만인 사업자, 그 외의 업종인 경우 상시근로자 수가 5인 미만인 사업자를 말함

▸ 상시근로자 : 「중소기업기본법 시행령」 제4조 및 제5조에 의거, 근로자 중에서 '임원', '일용근로자', '3개월 이내의 기간을 정하여 근로하는자', '기초연구진흥 및 기술개발지원에 관한 법률' 제14조에 해당하는 기업부설연구소의 연구전담요원을 제외한 근로자

11-1-2. 내부관리계획의 필수 반영사항(5개) 포함 여부

❍ 내부관리계획을 수립 시 보호책임자 지정 등 필수사항(5)을 모두 반영하여 수립하였는지 확인

< 내부관리계획 필수 항목(5) >

① 개인정보 보호책임자 지정에 관한 사항
② 개인정보 보호책임자 및 개인정보취급자의 역할·책임에 관한 사항
③ 개인정보의 안전성 확보에 필요한 조치에 관한 사항
④ 개인정보취급자에 대한 교육에 관한 사항
⑤ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
⑥ 그 밖에 개인정보 보호를 위하여 필요한 사항(예: 개인정보파일 보유기간 등)

개인정보 내부관리계획 목차 (예시)

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)

제3장 개인정보보호책임자의 의무와 책임
제6조(개인정보보호책임자의 지정)
제7조(개인정보보호책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적·관리적 안전조치
제9조(개인정보취급자 접근 권한 관리 및 인증)
제10조(접근통제)
제11조(개인정보의 암호화)
제12조(접근기록의 위변조 방지)
제13조(보안프로그램의 설치 및 운영)
제14조(물리적 접근제한)

제5장 개인정보보호 교육

제6장 수탁자에 대한 관리 및 감독에 관한 사항

제7장 개인정보 침해대응 및 피해구제

11-2 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	2.접근권한 관리 및 접근통제	11-2-1. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부			
		11-2-2. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부			
		11-2-3. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부			
		11-2-4. 취급자별로 개별 계정 발급 및 계정 미공유 여부			
		11-2-5. 안전한 비밀번호 작성규칙의 수립·적용 여부			
		11-2-6. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부			
		11-2-7. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부			
		11-2-8. 본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인			
		11-2-9. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부			
		11-2-10. 고유식별번호 처리시 연 1회 이상 취약점 점검 실시 여부			
		11-2-11. 업무용 모바일 기기에 비밀번호 설정 여부			

□ 점검 방법 및 평가 기준

11-2-1. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부

❍ 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 확인

- 업무 성격에 따라 접근 권한의 팀별, 개인별 차등 부여 여부 확인

☞ **개발 초기 시 부여된 관리자 권한, 디폴트 권한 등으로 일괄 부여된 사례 있음**

11-2-2. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부

❍ 개인정보취급자의 전보 또는 퇴직 등 인사이동 발생 시 개인정보처리시스템의 접근권한을 즉시 변경 또는 말소하는지 확인

☞ **퇴직자의 계정을 삭제하지 않고 남겨 놓은 사례 있음**

11-2-3. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부

❍ 개인정보취급자의 접근권한 부여 및 전보 또는 퇴직에 따른 변경, 말소에 대한 기록은 최소 3년간 보관하고 있는지 확인

※ 변경 이력을 시스템에 자동으로 남기지 않는 경우 수기로 작성, 관리 여부 확인

☞ **권한 변경 이력을 보관하지 않거나, 3년 미만으로 보관하는 사례 있음**

11-2-4. 취급자별로 개별 계정 발급 여부 및 계정 미공유 여부

❍ 개인정보처리시스템에 접속 할 수 있는 사용자 계정을 발급하는 경우, 취급자 별로 한 개의 사용자 계정을 발급하는지 확인

- 사용자 계정(ID)을 다수의 사용자가 공유하는지 여부 확인

☞ **업무 편의상 하나의 계정(ID)을 다수의 사용자가 공유하여 사용하는 사례 있음**

11-2-5. 안전한 비밀번호 작성규칙의 수립·적용 여부

❍ 개인정보취급자 또는 정부주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하는지 확인

※ 내부관리계획의 안전성확보 조치 사항으로 포함하여 작성 할 수 도 있으며, 별도 비밀번호 작성규칙을 작성하여 운영할 수 있음

< 안전한 비밀번호 작성 규칙>

o 최소 길이 - 최소 10자리 이상 : 영어 대문자, 소문자, 숫자, 특수문자 중 2종류 조합 - 최소 8자리 이상 : 영어 대문자, 소문자, 숫자, 특수문자 중 3종류 조합 o 추측하기 어려운 비밀번호 - 일련번호, 전화번호 등 쉬운 문자열이 포함되지 않도록 함 - 잘 알려진 단어, 키보드 상에서 나란히 있는 문자열이 포함되지 않도록 함 o 주기적 변경 : 비밀번호에 유효기간 설정하고 최소 6개월마다 변경 o 동일 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않음

☞ **비밀번호 작성규칙에 불구하고 취급자 등이 시스템 접속 시 반영하지 않은 사례 있음**

11-2-6. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부

❍ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근통제시스템*을 설치 운영하는지 확인

* · 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 시스템(방화벽 등)
· 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템(IDS 또는 IPS 등)

※ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우, 접근통제시스템을 적용하지 아니할 수 있음. 단, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용 가능

☞ **웹호스팅 시 방화벽 등 보안장비 이용에 추가 비용이 들어 설치하지 않은 사례 있음**

11-2-7. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부

❍ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 안전한 접속수단(가상사설망(VPN), 전용선 등)을 통해서만 접속하는지 확인

☞ **홈페이지 관리자페이지 접속 시 단순 ID/패스워드로만 접속 가능한 사례 있음**

11-2-8. 본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인

❍ 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인*하여야 함

* 추가적인 정보를 확인하는 방법에는 I-PIN, 공인인증서, 휴대전화, 주민등록증 발급 일자, 전자우편(e-mail) 주소 등이 있음

☞ **성명, 주민등록번호 만을 이용해서 본인확인하는 경우 공격의 대상이 되는 사례 있음**

11-2-9. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부

❍ P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 PC에 조치를 취하고 있는지 확인

❍ 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 PC 및 모바일 기기* 등에 조치를 취해야함

* 스마트폰, 스마트패드, 태블릿PC 등

☞ **업무용 모바일 기기의 분실에 따라 개인정보 유출되는 사례 있음**

※ 모바일 기기(스마트폰, 스마트패드, 태블릿PC 등)의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 보호조치(비밀번호, 패턴, PIN 등 설정) 필요

❍ 「홈페이지 개인정보 노출방지 가이드라인」에서 제시하고 있는 관리적, 기술적 노출방지 대책을 적용하고 있는지 확인

* 개인정보보호포털(http://www.privacy.go.kr)의 〔자료실-지침자료〕에서 확인 가능

☞ **웹서버 설정이 미흡하여 게시판 등에 올린 개인정보가 구글 등에 노출되는 사례 있음**

※ 홈페이지 개발 및 운영 단계에서 웹 취약점 점검, 미관리 사이트 및 URL 차단 및 삭제, 관리자 페이지 노출 차단 등의 조치 시행 필요

11-2-10. 고유식별번호 처리시 연 1회 이상 취약점 점검 실시 여부

❍ 인터넷 홈페이지를 통해 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)를 처리하는 개인정보처리자는 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고, 취약점에 대한 개선조치를 취하여야 함

☞ **홈페이지 취약점으로 인해 고유식별정보가 유출되는 사례 있음**

11-2-11. 업무용 모바일 기기에 비밀번호 설정 여부

❍ 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치*를 하여야 함

* 비밀번호, 패턴, PIN 등을 이용한 화면잠금, 디바이스 암호화, USIM 카드 잠금 설정, 원격 잠금 및 데이터 삭제 등

☞ **업무용 모바일 기기의 분실에 따라 개인정보 유출되는 사례 있음**

11-3 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	3.개인정보의 암호화	11-3-1. 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호화 조치 여부			
		11-3-2. 비밀번호 및 바이오정보의 저장 시 암호화 조치 여부 (단, 비밀번호의 경우 일방향 암호화)			
		11-3-3. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부			
		11-3-4. 고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부			
		11-3-5. 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인			
		11-3-6. 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인			

□ 점검 방법 및 평가 기준

11-3-1. 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달 시 암호화 조치 여부

❍ 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 내·외부로 송·수신하거나 보조저장매체 등을 통해 전달하는 경우에 이를 암호화하는지 확인

☞ **내부망 내에서 송·수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화해야 함**

☞ **암호화 대상인 개인정보를 전용선을 통해 송수신 시, 반드시 암호화할 필요는 없음**

☞ **wire shark 등 프로그램을 통해 전송되는 패킷의 암호화 검사 시 암호화하지 않은 사례 있음**

- **(붙임) 「네트워크 전송 구간 암호화 여부 검사 방법(WireShark 사용법)」 참고**

11-3-2. 비밀번호 및 바이오정보의 저장 시 암호화 조치 여부 (단, 비밀번호의 경우 일방향 암호화)

❍ 비밀번호 및 바이오정보*를 저장 시 암호화하는지 확인

*식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외

❍ 특히, 비밀번호는 복호화 되지 않도록 일방향 암호화(해시함수)하여 저장하는지 확인

11-3-3. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부

❍ 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인

11-3-4. 고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부

❍ 내부망에 고유식별정보를 저장하는 경우에는 암호화의 적용여부 및 적용범위를 정하여 시행하고 있는지 확인

- 영향평가 대상이 되는 공공기관의 경우 개인정보영향평가의 결과에 따라 암호화 적용여부 및 범위를 정할 수 있음
- 영향평가 대상이 되는 공공기관의 경우를 제외하고는 위험도 분석에 따른 결과에 따라 암호화 적용여부 및 범위를 정함

< 개인정보 영향평가의 대상 >

① 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일

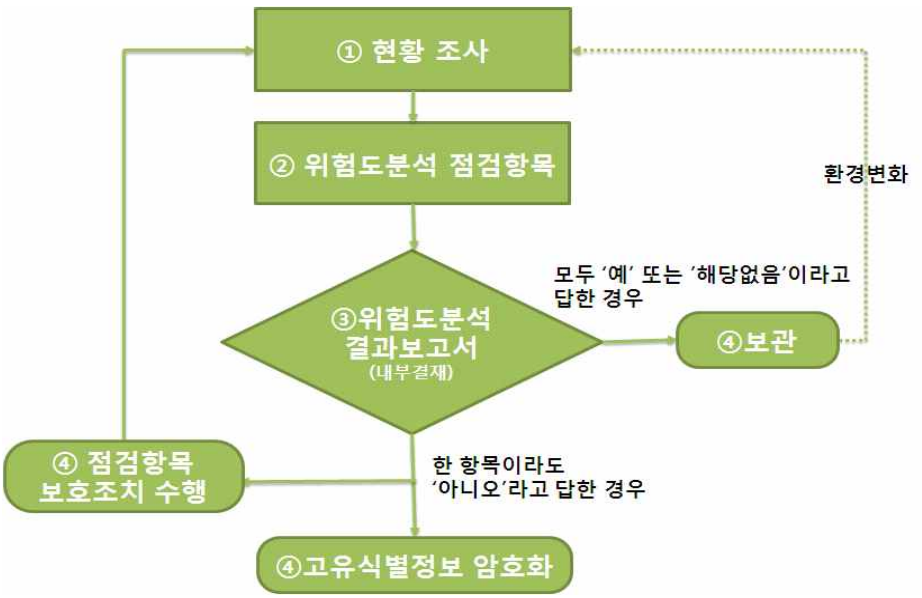
② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

④ 법 제33조 제1항에 따른 개인정보영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일

< 위험도 분석 절차 및 내용 >

① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행
③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
④ 점검 결과에 따라 고유식별정보 암호화 등을 수행



구 분	점 검 항 목
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB서버 내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사이동 발생 시 지체 없이 DB 접근권한을 변경하고 있습니까?
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?
	20. DB접속자 및 개인정보취급자의 비밀번호 입력 시 5회 이상 연속 입력오류가 발생한 경우 계정 잠금 등 접근을 제한하고 있습니까?

	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?
	24. HDD등 DB 저장매체의 불용 처리 시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹(Web) 기반 ※웹사이트 운영시	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?

11-3-5. 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인

❍ 개인정보처리시스템에 고유식별정보, 비밀번호, 바이오정보를 암호화하여 저장 시, 안전한 암호알고리즘을 사용해야함

- 안전한 암호알고리즘, 암호화 방식 등은 “개인정보 암호화 조치 안내서” 참조

  * 개인정보보호 종합지원포털(http://www.privacy.go.kr)에서 다운로드 가능

☞ **안전한 암호알고리즘을 사용하더라도 암호화 키가 잘못 관리되어 유노출 되는 경우에는 암호화된 정보들이 유노출될 수 있으므로 이를 안전하게 관리하여야 함**

11-3-6. 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인

❍ 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용

- 안전한 암호알고리즘, 암호화 방식 등은 “개인정보 암호화 조치 안내서” 참조

  * 개인정보보호 종합지원포털(http://www.privacy.go.kr)에서 다운로드 가능

☞ **안전하지 않은 알고리즘(MD5, SHA-1, 자체 함수제작 등) 및 양방향 암호화 방식으로 암호화한 사례 있음**

11-4 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	4.접속기록의 보관	11-4-1. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부			
		11-4-2. 접속기록의 항목(4개*)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행 업무(열람, 수정, 삭제, 인쇄, 입력 등)			
		11-4-3. 접속기록 정기 점검			
		11-4-4. 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부			

□ 점검 방법 및 평가 기준

11-4-1. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부

❍ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는지 확인

☞ **홈페이지 관리자 페이지 접속 시 접속 기록을 남기지 않은 사례 있음**

11-4-2. 접속기록의 항목(4개)이 적정한지 여부

❍ 개인정보처리시스템에 접속 시 필수항목(4)을 남기는지 확인

< 접속기록에 포함되어야 할 필수 항목 >

필수 기록 항목	설 명
① ID	개인정보취급자 식별 정보
② 날짜 및 시간	접속 일시
③ 접속자 IP 주소	접속지 정보
④ 수행 업무	열람, 수정, 삭제, 입력, 인쇄 등

※ 개인정보취급자 1명(Root, Admin 등)이 개인정보처리시스템을 관리하는 경우, 전자적 로그를 남기지 않고, 접속 기록을 수기로 작성하여 상급자의 승인을 받아도 가능

11-4-3. 접속기록 정기 점검

❍ 개인정보의 유출·변조·훼손 등에 대응하기 위해 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하는지 여부 확인

11-4-4. 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부

❍ 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하고 있는지 확인

- 접속기록에 대한 위·변조를 방지하기 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직함

- 접속기록을 수정 가능한 매체(HDD 또는 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음

11-5 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	5.보안프로그램 설치·운영	11-5-1. 보안 프로그램의 설치·운영 여부			
		11-5-2. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부			

□ 점검 방법 및 평가 기준

11-5-1. 보안 프로그램의 설치·운영 여부

❍ 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 있는지 확인

11-5-2. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부

❍ 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하고 있는지 확인

- 악성 프로그램관련 경보가 발령된 경우
- 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 업데이트를 하고 있는지 확인

☞ **백신프로그램 업데이트 및 OS 최신 패치 확인 시 업데이트를 미실시하는 사례 있음**

11-6 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야		세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	6.물리적 접근 방지	11-6-1. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부			
		11-6-2. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부			

□ 점검 방법 및 평가 기준

11-6-1. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부

❍ 전산실·자료보관실을 별도로 두고 있는 경우에는 비인가자의 접근으로 인한 개인정보의 절도, 파괴 등의 물리적 위협으로부터 정보자산을 보호하기 위해 출입통제 절차를 수립하는지 확인

- 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입 통제장치 등 물리적 접근통제 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하고 있는지 확인

11-6-2. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부

※ 별도의 개인정보처리시스템을 운영하지 아니하고, 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 해당없음에 체크

❍ 개인정보가 포함된 서류나 보조기억매체(USB, CD 등) 등은 잠금장치가 부착되어 있는 금고 또는 잠금장치가 있는 캐비넷 등에 안전하게 보관하고 있는지 확인

☞ **개인정보가 포함된 서류 등을 캐비넷에 보관하지 않고 책상에 방치하는 사례 있음**

12 개인정보 처리방침의 수립·공개 (법 제30조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제30조(개인정보 처리 방침의 수립·공개)	12-1. 개인정보 처리방침의 수립 여부			
	12-2. 개인정보 처리방침에 필수 항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁 사항(해당 시), 정보주체 권리·의무 및 행사 방법, 처리 항목, 파기 사항, 안전성 확보 조치 사항			
	12-3. 개인정보 처리방침의 홈페이지 등 공개 여부			

□ 점검 방법 및 평가 기준

12-1. 개인정보 처리방침의 수립 여부

❍ 개인정보 처리에 관한 '개인정보처리방침'을 수립하고 있는지 확인

12-2. 개인정보 처리방침에 필수 항목(8개) 포함 여부

❍ 개인정보처리방침 공개 시 필수 항목을 포함하여 공개하는지 확인

< 개인정보처리 방침 필수 항목 >

① 개인정보의 처리 목적	② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항	④ 개인정보 처리의 위탁에 관한 사항
⑤ 정보주체의 권리·의무 및 행사방법에 관한 사항	
⑥ 처리하는 개인정보의 항목	⑦ 개인정보의 파기에 관한 사항
⑧ 안전성 확보 조치에 관한 사항	

12-3. 개인정보 처리방침의 홈페이지 등 공개 여부

❍ '개인정보처리방침'을 홈페이지에 공개해고 있는지, 홈페이지가 없는 경우 사업장의 보기 쉬운 장소에 게시하는 방식 등으로 공개하는지 확인

13 개인정보 보호책임자의 지정 (법 제31조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제31조(개인정보 보호 책임자의 지정)	13-1. 개인정보 보호책임자 지정 여부			

□ 점검 방법 및 평가 기준

13-1. 개인정보 보호책임자 지정 여부

❍ 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호 책임자를 지정하고 있는지 확인

- 민간 사업자는 대표자, 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람을 개인정보 보호책임자로 지정하고 있는지 확인

- 공공기관은 다음의 자격 요건에 맞게 지정하고 있는지 확인

< 공공기관 개인정보보호책임자 자격 요건 >

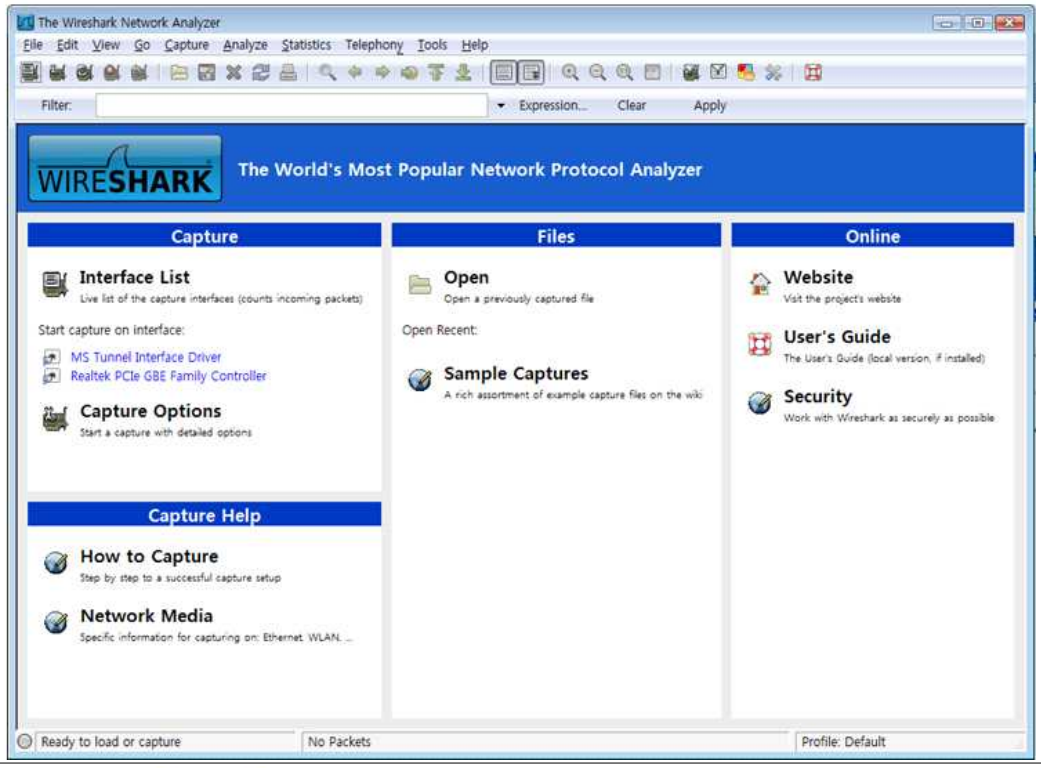
공공 기관		자격 요건
①	국회, 법원, 헌법재판소, 중앙선관위, 중앙행정기관	고위공무원단
②	① 외 정무직공무원을 장으로 하는 국가기관	3급 이상 공무원
③	①, ② 외 고위·3급 공무원을 장으로 하는 국가기관	4급 이상 공무원
④	①~③ 외의 국가기관	개인정보 처리 업무 담당 부서장
⑤	시·도 및 시·도 교육청	3급 이상 공무원
⑥	시·군· 및 자치구	4급 이상 공무원
⑦	각급 학교	행정사무 총괄자
⑧	①~⑦ 외 공공기관	개인정보 처리 업무 담당 부서장

☞ **개인정보파일을 운영하면서 개인정보 보호책임자를 지정하지 않는 사례 있음**

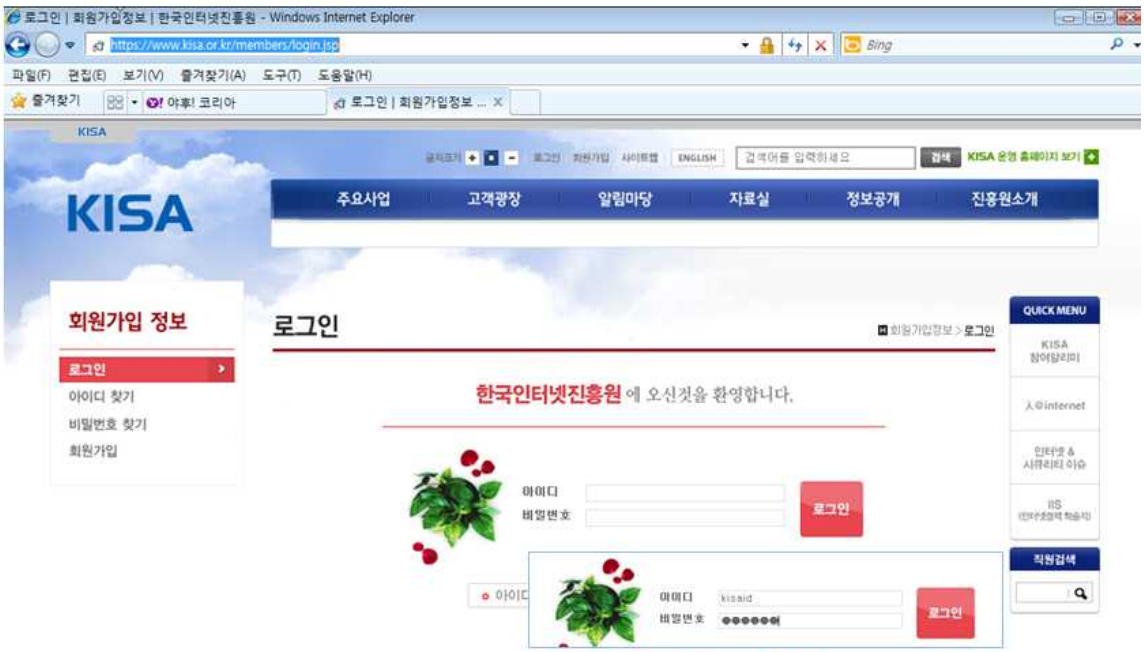
붙임1 네트워크 전송 구간 암호화 여부 검사 방법(wireshark 사용법)

※ WireShark 프로그램은 프리웨어로 인터넷에 검색하여 설치 할 수 있음(출처:KISA)

① WireShark 구동

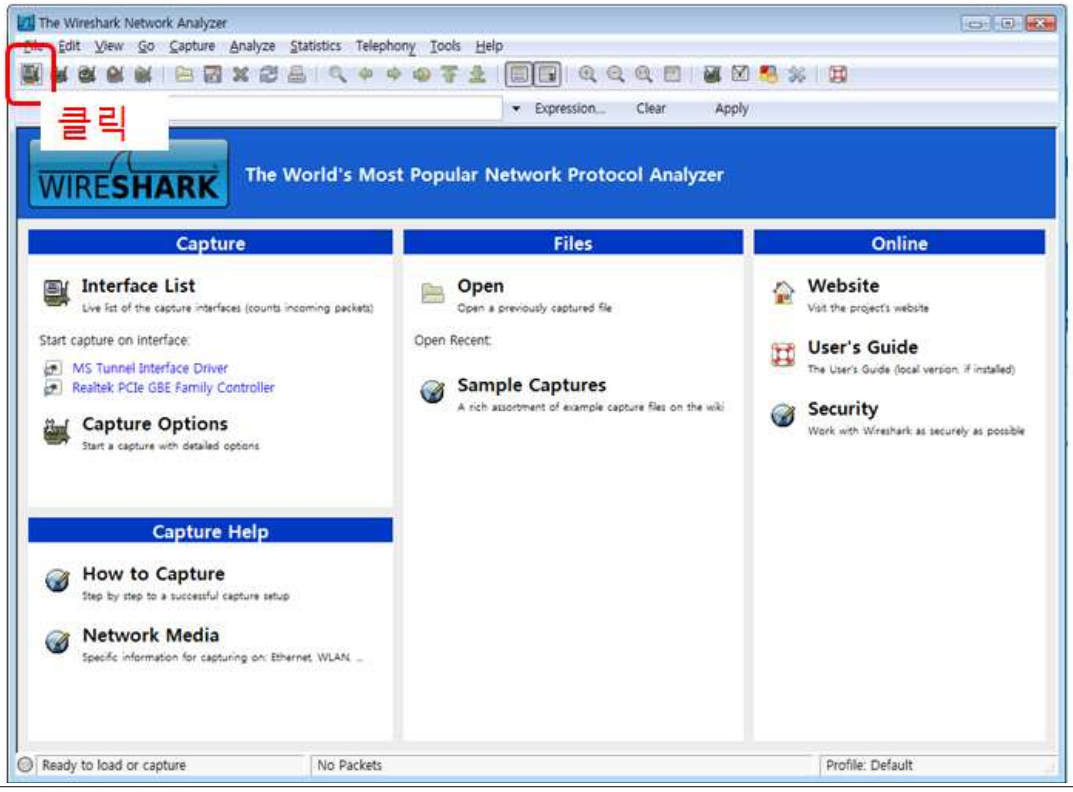


② 점검대상 웹페이지 접속(ex: https://www.kisa.or.kr/members/login.jsp)

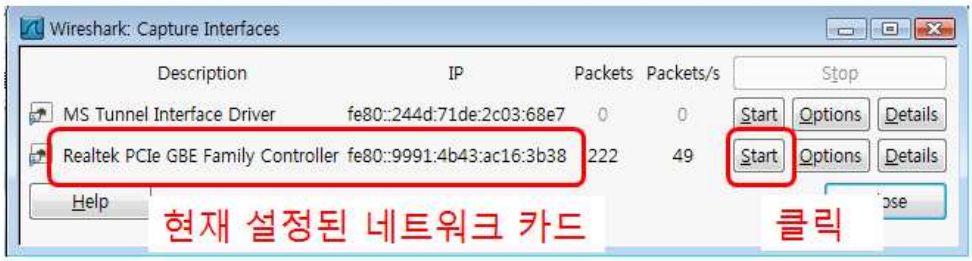


③ 암호화 필요정보 입력
(ex: ID는 kisaid, PW는 kisapw)

③ 패킷캡쳐 인터페이스 설정



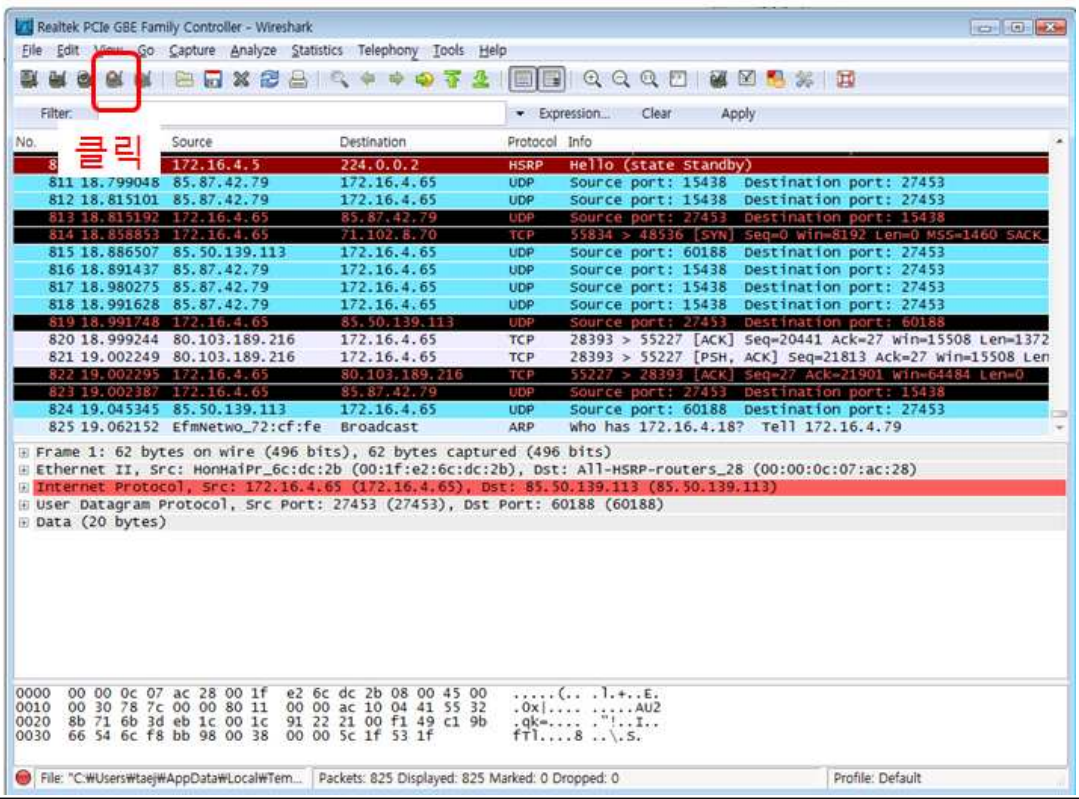
④ 패킷캡쳐 시작



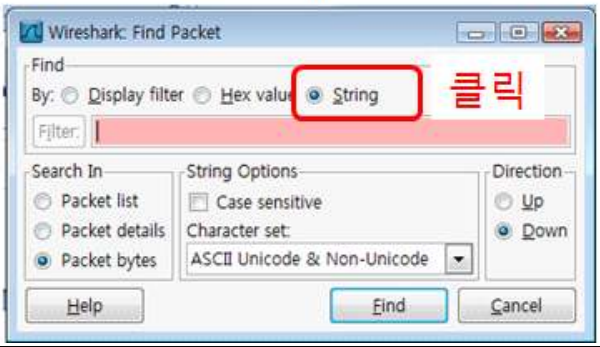
※ packets/s의 수치가 증가하는 것이 현재 설정된 네트워크 카드임

⑤ 점검대상 웹페이지에서 패킷발송(ex: 로그인 버튼 클릭)

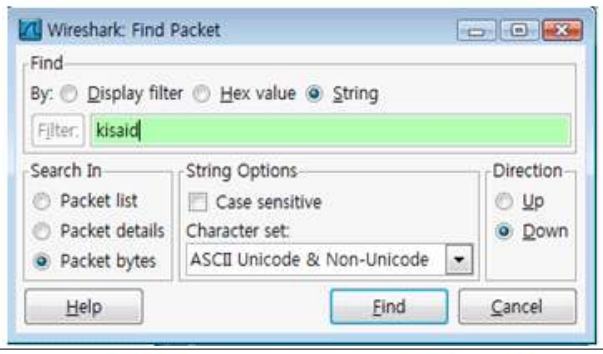
⑥ 캡쳐된 패킷을 확인 (ex: 로그인 버튼 클릭)



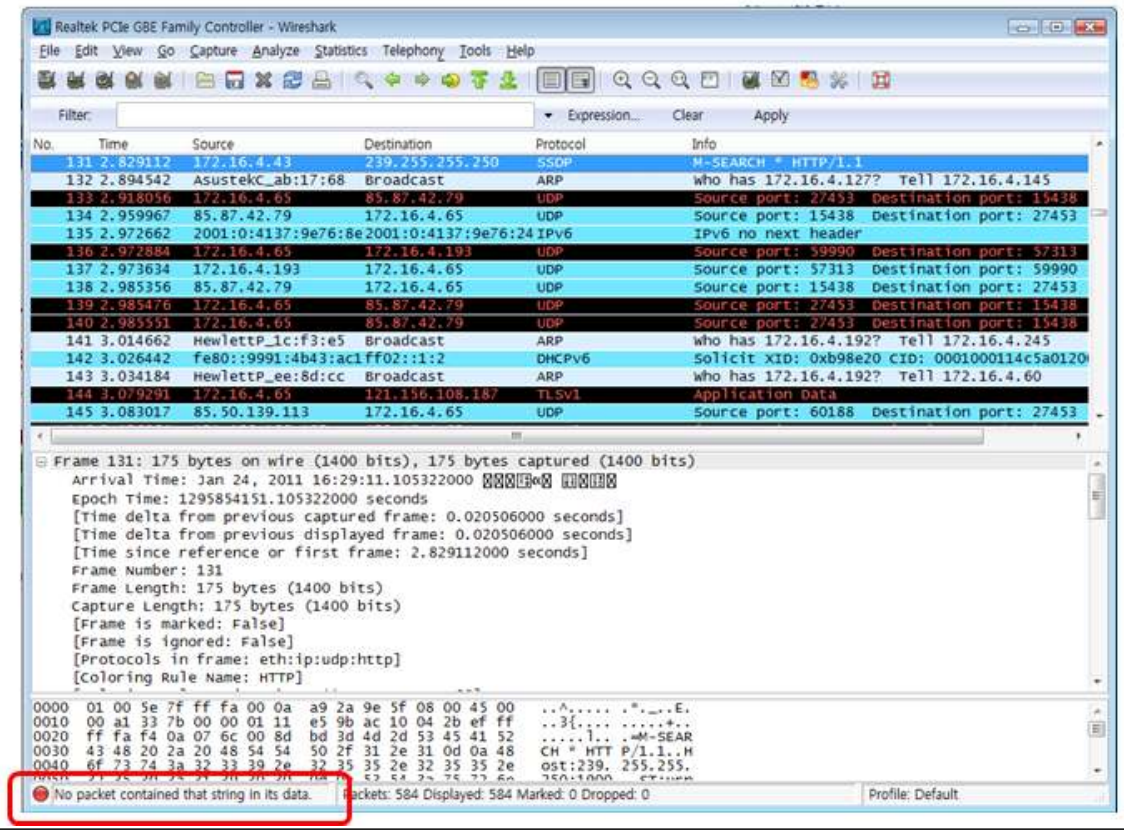
⑦ 캡쳐된 패킷의 확인화면(⑦)에서 단축키 Ctrl + F 클릭



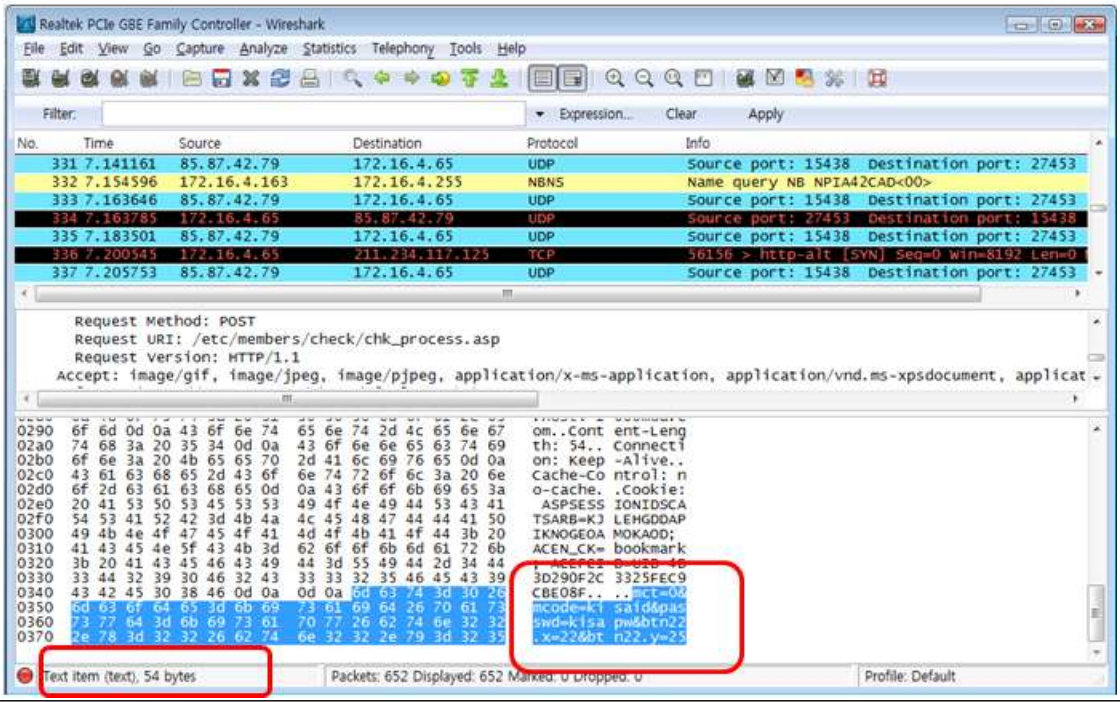
⑧ 암호화 필요 정보 입력 (③의 문자열 입력)



⑨ 암호화 된 정보는 검색이 되질 않음을 확인



⑩ 암호화가 되지 않은 경우 ID(kisaid), PW(kisapw) 확인 가능



경기도 조례, 매뉴얼

경기도 개인정보 보호 조례

(제정) 2012-05-11 조례 제 4386호
(일부개정) 2013-08-05 조례 제 4576호 (경기도 조례 중 중앙행정기관 명칭 등 일괄정비 조례)
(일부개정) 2014-03-05 조례 제 4692호
(일부개정) 2014-10-21 조례 제 4780호 (경기도 조례 중 주민등록번호 처리에 관한 일괄정비 조례)
(일부개정) 2015-01-05 조례 제 4817호 (경기도 출자․출연 기관의 운영에 관한 기본조례)
(일부개정) 2015-04-30 조례 제 4898호 (경기도 조례 용어 등 일괄정비 조례)

제1조(목적) 이 조례는「개인정보 보호법」및 같은 법 시행령·시행규칙에서 위임한 사항 등 경기도의 개인정보 보호업무에 필요한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 조례에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.5.>

1. “공공기관”이란 경기도(이하 “도”라 한다)가 설립한 공사·공단 및 「경기도 출자·출연기관의 운영에 관한 기본조례」 제2조제1호 또는 제16조에 해당하는 출자·출연·보조 법인 또는 기관을 말한다. <개정 2015.1.5.>
2. “총괄부서”란 도 개인정보 보호업무를 주관하는 담당 부서를 말한다. <개정 2014.3.5.>

제3조(개인정보 보호책임자 등의 지정) ① 「개인정보 보호법」(이하 “법”이라 한다)제31조 및 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제32조제2항제1호에 따른 개인정보 보호책임자와 그 밖의 관리책임자 등은 다음 각 호의 구분에 따라 도지사가 지정한다. <개정 2014.3.5.>

1. 개인정보 보호책임자 및 영상정보 보호책임자 : 기획조정실장
2. 개인정보 관리책임자 : 개인정보 파일을 보유한 부서의 장
3. 영상정보 관리책임자 : 영상정보처리기기를 설치하고 운영하는 부서의 장

② 공공기관의 개인정보 보호책임자·영상정보 보호책임자, 개인정보 관리책임자·영상정보관리책임자는 공공기관의 장이 정하고, 경기도지사(이하 “도지사”라 한다)에게 보고한다.

제4조(개인정보 보호담당자의 지정) ① 도지사는 제3조제1항에 따라 지정된 개인정보 보호책임자의 업무를 보조하기 위하여 총괄부서에 개인정보 보호 업무만을 전담하는 개인정보 보호담당자를 1명 이상 지정하여야 한다.

② 공공기관의 장은 제3조제2항에 따라 지정된 개인정보 보호책임자의 업무를 보조하기 위하여 개인정보 보호담당자를 1명 이상 지정하여야 한다.

제5조(개인정보파일 관리) ① 영 제34조에 따라 도 및 공공기관의 개인정보 관리책임자는 개인정보파일 운용을 시작한 날부터 60일 이내에 총괄부서를 통하여 행정자치부장관에게 등록을 신청하여야 한다. 등록 후 등록사항이 변경된 경우에도 또한 같다. <개정 2013.8.5., 2015.4.30.>

② 총괄부서의 장은 개인정보파일의 등록·변경 사항을 검토하고 그 적정성을 판단하며, 등록사항과 내용의 흠이 확인된 경우 개선사항을 권고하고, 이를 시정하여 재신청하도록 하여야 한다. 다만, 내부적 업무처리만을 위하여 사용되는 개인정보파일 및 개인영상정보, 그 밖에「통계법」에 따라 수집되는 개인정보파일 등은 법령에 따라 등록 신청 대상에서 제외한다.

③ 개인정보 관리책임자는 개인정보파일을 파기한 경우 총괄부서를 통하여 행정자치부장관에게 개인정보파일의 등록사항에 대한 삭제를 요청하여야 한다. <개정 2013.8.5., 2015.4.30.>

제6조(개인정보 유출에 따른 대책) ① 개인정보 관리책임자는 개인정보가 유출된 사실을 알게 된 경우에는 특별한 사유가 없으면 지체 없이 정보주체에게 법 제34조제1항 각 호의 사항을 알려야 한다.

② 1만명 이상인 정보주체의 개인정보가 유출된 경우에는 서면, 전자우편 등의 방법과 함께 인터넷 홈

페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

③ 개인정보 관리책임자는 개인정보가 유출되었을 경우 별지 제1호서식의 개인정보 유출신고서를 작성하여 총괄부서로 제출하여야 한다.

④ 총괄부서의 장은 개인정보 유출사고에 대하여 기술적 분석 작업 및 점검을 실시할 수 있다.

제7조(수수료 청구 및 납부) ① 도지사 및 공공기관의 장은 법 제38조제3항 및 영 제47조제1항에 따라 정보주체(법 제38조의 대리인을 포함한다)에게 법 제35조에 따른 열람의 요구, 제36조에 따른 정정·삭제의 요구, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)에 따라 발생하는 수수료 및 우송료를 별표에 따라 청구할 수 있다. 다만, 영 제47조제2항에 따라 열람등요구를 하게 된 사유가 도 및 공공기관에 있는 경우에는 제1항에 따른 수수료 및 우송료를 청구할 수 없다.

② 도 및 공공기관이 제1항의 수수료 또는 우송료를 받을 때에는 영 제47조제3항에 따라 수입증지 또는「전자금융거래법」제2조제11호에 따른 전자지급수단을 이용하여 받을 수 있다.

③ 이미 납부한 비용은 개인정보 열람 등이 처리되기 전에 그 신청을 취소하면 반환하여야 한다. 다만, 소인된 수입증지는 제외한다.

제8조(이의신청) ① 정보주체는 법 제38조제5항에 따른 열람등요구에 대한 거절 등의 조치에 불복이 있는 경우에는 거절 등의 통보를 받은 날부터 30일 이내에 별지 제2호서식의 개인정보 열람등요구 결정 이의신청서로 이의신청을 할 수 있다.

② 도지사 및 공공기관의 장은 제1항의 이의신청을 받은 날부터 14일 이내에 심의위원회의 회의에 부쳐 심의·결정하여야 한다. 다만, 부득이한 사유로 정해진 기간 이내에 처리할 수 없는 경우에는 그 기간의 만료일 다음 날부터 7일 이내의 범위에서 연장할 수 있으며, 연장사유를 별지 제3호서식의 이의신청 결정기간 연장 통지서로 이의신청을 한 정보주체에게 통지하여야 한다.

③ 도지사 및 공공기관의 장은 심의·결정을 한 후 해당 절차에 따라 특별한 사유가 없는 한 5일 이내에 이의신청을 한 정보주체에게 별지 제4호서식의 이의신청 결정 통지서로 통보하여야 한다.

제9조(개인정보 보호 심의위원회의 설치) 다음 각 호의 사항을 심의하기 위하여 도에 개인정보 보호 심의위원회(이하 "심의위원회"라 한다)를 둘 수 있다.

1. 제8조의 이의신청에 대한 사항
2. 개인정보 보호에 관한 시책 및 제도개선에 관한 사항
3. 그 밖에 개인정보 보호와 관련하여 개인정보 보호책임자가 심의에 부치는 사항

제10조(심의위원회의 구성 및 운영) ① 심의위원회의 위원은 위원장을 포함하여 11명 이내로 구성한다.

② 심의위원회의 위원장은 개인정보 보호책임자가 되고, 위원은 다음 각 호와 같으며, 제2호의 위촉직 위원은 한 쪽의 성(性)이 100분의 60을 넘지 아니하도록 노력하여야 한다. <개정 2014.3.5.>

1. 당연직 위원 : 정보화업무 담당 국장, 감사업무 담당 과장, 조사업무 담당 과장, 법무업무 담당 과장, 기획예산업무 담당 과장, 총괄부서의 장 <개정 2014.3.5.>
2. 위촉직 위원 : 개인정보에 관한 학식과 경험이 풍부한 외부전문가. 이 경우 4명까지 위촉할 수 있다. <개정 2014.3.5.>

③ 위원장은 개인정보 보호책임자가 되고, 위원장이 부득이한 사유로 직무를 수행할 수 없을 경우에는 도의 당연직 위원 중 직제순에 따라 그 다음 순위자가 그 직을 대행한다.

④ 위원은 심의위원회를 개최할 때마다 도지사가 임명 또는 위촉하고, 회의가 끝난 후에 임명 또는 위촉이 해제된 것으로 본다.

⑤ 심의위원회의 회의는 재적위원 과반수의 출석으로 열고, 출석위원 과반수의 찬성으로 의결한다.

⑥ 삭제 <2014.3.5.>

제10조의2(위원의 제척·기피·회피 등) ① 위원은 심의·의결의 공정성을 도모하기 위하여 자기와 직접 이해관계가 있는 안건의 심의·의결에는 관여할 수 없다.

② 위원은 제1항에 따른 제척사유가 있거나 심의·의결의 공정을 기대하기 어려운 사유가 있는 경우 관계인의 기피신청에 따라 심의·의결에서 제외될 수 있다.

③ 위원은 제척 또는 기피사유에 해당하는 경우 스스로 심의·의결을 회피할 수 있다.

[본조신설 2014.3.5.]

제10조의3(간사) 심의위원회의 사무를 처리하기 위하여 심의위원회에 간사 1명을 두되, 간사는 총괄부서의 개인정보 보호업무 담당 팀장이 된다.

[본조신설 201.3.5.]

제11조(안건 상정) ① 제9조 각 호의 안건을 심의위원회의 회의에 부치려는 경우에는 별지 제5호서식의 개인정보 보호 심의위원회 심의요청서를 심의위원회의 간사에게 제출하여야 한다.

② 간사는 심의 전에 법무업무 담당 부서, 감사업무 담당 부서 및 총괄부서의 의견을 듣고, 별지 제6호서식의 개인정보 보호 심의위원회 이의신청 심의조서를 작성하여 심의위원회에 심의를 요구하여야 한다.

③ 간사는 심의위원회에 참석하여 별지 제7호서식의 개인정보 보호 심의위원회 심의의결서 및 별지 제8호서식의 회의록을 작성하여야 한다.

제12조(결과 통보) 위원장은 심의위원회에서 의결된 사항을 제11조제1항에 따라 심의요청을 한 자에게 통지하여야 한다.

제13조(수당 등) 심의위원회의 회의에 출석한 위촉직 위원 및 그 밖의 참고인에게는 「경기도위원회실비변상조례」 및 예산의 범위에서 정하는 바에 따라 여비와 수당 등을 지급할 수 있다.

제14조(보험·공제 등의 가입) 도지사 및 공공기관의 장은 개인정보를 취급하는 업무 중 개인정보 침해사고에 따른 피해발생과 이로 인한 손해배상에 대비하기 위하여 보험 또는 공제 등에 가입할 수 있다.

부칙 <2012.05.11.>

이 조례는 공포한 날부터 시행한다.

부칙(경기도 조례 중 중앙행정기관 명칭 등 일괄정비 조례) <제4576호, 2013.08.05.>

이 조례는 공포한 날부터 시행한다.

부칙 <2014.3.5.>

이 조례는 공포한 날부터 시행한다.

부칙(경기도 조례 중 주민등록번호 처리에 관한 일괄정비 조례) <제4780호, 2014.10.21.>

이 조례는 공포한 날부터 시행한다.

부칙(경기도 출자·출연 기관의 운영에 관한 기본조례) <제4817호, 2014.01.05.>

제1조(시행일)이 조례는 공포한 날부터 시행한다.

제2조(다른 조례의 폐지)「경기도 공공기관 경영평가 등에 관한 조례」는 폐지한다.

제3조(다른 조례의 개정)① 경기도 개인정보 보호 조례 일부를 다음과 같이 개정한다.

제2조제1호 중 “「경기도 공공기관 경영평가 등에 관한 조례」 제2조제1호에 따라 경기도(이하 “도”라 한다)가 출자·출연·보조한 법인 또는 기관”을 “경기도(이하 “도”라 한다)가 설립한 공사·공단 및 「경기도 출자·출연기관의 운영에 관한 기본조례」 제2조제1호 또는 제16조에 해당하는 출자·출연·보조 법인 또는 기관”으로 한다.

②~⑧ 생략

부칙(경기도 조례 용어 등 일괄정비 조례) <제4898호, 2015.04.30.>

이 조례는 공포한 날부터 시행한다.

경기도 개인영상정보 보호 및 영상정보처리기기 설치·운영 조례

(제정) 2016-07-19 조례 제 5277호

제1조(목적) 이 조례는 「개인정보 보호법」제25조에 따라 경기도 관내 영상정보처리기기의 설치·운영에 관한 사항 및 개인영상정보 보호에 필요한 사항을 정함으로써 경기도민의 개인정보자기결정권을 보장하고 개인의 자유와 권리를 보호함을 목적으로 한다.

제2조(용어의 정의) 이 조례에서 사용하는 용어의 정의는 다음과 같다.

1. “영상정보처리기기”란 「개인정보 보호법」(이하 “법”이라 한다.) 제2조제7호에 따른 장치로서 법 시행령 제3조의 폐쇄회로텔레비전(CCTV) 및 네트워크카메라를 말한다.
2. “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
3. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
4. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
5. “공개된 장소”란 공원, 도로, 지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용대상 등) ① 이 조례는 법 제25조제1항 각 호에 따라 경기도(이하 “도”라 한다) 관내의 공개된 장소에 설치·운영하는 영상정보처리기기와 이를 통하여 처리되는 개인영상정보를 적용대상으로 한다.

② 적용대상에 관하여는 다른 조례에 특별한 규정이 있는 경우 외에는 이 조례에서 정하는 바에 따른다.

제4조(개인영상정보의 보호원칙) ① 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기 운영자”라 한다)는 영상정보처리기기 설치목적의 최소한의 범위에서 개인영상정보를 수집하여야 한다.

② 제1항의 영상정보처리기기 설치목적은 누구나 쉽게 인식할 수 있도록 명확히 하여야 하며, 수집된 개인영상정보는 그 설치목적 이외의 용도로 활용하여서는 아니 된다.

③ 영상정보처리기기 운영자는 영상정보처리기기 운영·관리방침 등 개인영상정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

④ 영상정보처리기기 운영자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인영상정보를 처리하여야 한다.

⑤ 영상정보처리기기 운영자는 개인영상정보 접속기록, 영상정보처리기기 조작행위기록을 남기고 소명처리 하여야 한다.

⑥ 영상정보처리기기 운영자는 개인영상정보의 오·남용 및 영상정보처리기기 임의조작행위를 예방하기 위한 영상정보내부통제시스템을 구축하여야 한다.

제5조(책무) ① 경기도지사(이하 “도지사”라 한다)는 정보주체의 권리가 침해되지 않도록 개인영상정보의 활용과 보호에 관한 시책을 마련하여야 한다.

② 도지사는 정보주체의 사생활 침해 소지가 있는 개인영상정보 처리의 사회적 관행 개선에 앞장서야 한다.

③ 관내 영상정보처리기기 운영자는 법에서 정한 개인영상정보 보호원칙을 준수하여야 한다.

제6조(영상정보처리기기의 관리계획) ① 도지사는 개인영상정보의 보호를 위하여 영상정보처리기기

관리에 관한 계획(이하 “관리계획”이라 한다)을 3년마다 수립하여야 한다.

② 관리계획에는 다음 각 호의 사항을 포함하여야 한다.

1. 관내 영상정보처리기기 설치·운영 현황 및 관리 방향
2. 영상정보처리기기의 관리에 대한 민관 협력체계 구축
3. 개인영상정보의 보호 방안 및 내부통제시스템의 구축
4. 개인영상정보의 보호에 대한 교육 및 홍보
5. 그 밖에 개인영상정보의 보호를 위하여 필요한 사항

③ 도지사는 수립된 관리계획을 도 홈페이지에 공개하여야 한다.

제7조(실태조사) ① 도지사는 관내 영상정보처리기기 설치·운영 현황을 파악하기 위하여 실태조사를 실시할 수 있다.

② 도지사는 관내 영상정보처리기기 운영자에게 실태조사에 필요한 자료제공을 요청할 수 있다.

제8조(교육 및 홍보) ① 도지사는 영상정보처리기기가 개인영상정보의 보호 원칙에 맞게 설치·운영될 수 있도록 준수사항 등에 관하여 영상정보처리기기 운영자 및 소속 공무원에게 지속적인 교육을 실시할 수 있다.

② 도지사는 영상정보처리기기에 의한 사생활 침해를 방지하고 개인영상정보의 보호에 대한 도민의식을 함양을 위하여 교육과 홍보를 실시할 수 있다.

제9조(시정명령 등) 도지사는 영상정보처리기기가 법 제25조에 반하여 설치·운영되고 있음을 발견한 경우 도 또는 산하기관이 직접 설치·운영하거나 도비가 지원되어 설치·운영하는 경우는 시정명령을 내릴 수 있고, 그 밖의 경우에는 해당기관 등이 시정할 수 있도록 위반사항을 안내하여야 한다.

제10조(협력 등) 도지사는 도내 영상정보처리기기의 효율적 관리를 위하여 시장·군수, 민간 영상정보처리기기 운영자, 경기남·북부지방경찰청, 경기교육청 등과 공동으로 관리계획을 추진하거나 협력할 수 있다.

제11조(시행규칙) 이 조례의 시행에 관하여 필요한 사항은 규칙으로 정한다.

부 칙 <2016.07.19.>

이 조례는 공포한 날부터 시행한다.

Global Inspiration
세계속의 경기도

경기도 개인정보 목적 외 이용·제공 절차서

경 기 도
(기획조정실)

개 정 이 력

[개인정보 목적 외 이용·제공 절차서]

개정번호	일 자	개 정 내 용	비고
1	2014.01.24.	절차서 제정	
2	2015.06.16.	절차서 1차 개정	

경기도 개인정보 목적 외 이용·제공 절차서

1. 목적

개인정보의 목적 외 이용·제공시 「개인정보보호법」에 따른 의무사항을 준수하고, 보유하고 있는 개인정보를 보호하는데 그 목적이 있다.

2. 용어의 정의

2.1 **제3자** : 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적·직접적으로 수집·보유한 개인정보처리자를 제외한 모든 자를 말한다.

2.2 **제3자 제공** : 제3자에게 개인정보의 지배·관리권이 이전되는 것으로 道에서 보유하고 있는 개인정보를 제3자에게 저장매체 저장 또는 개인정보가 담긴 출력물 등의 이전, 네트워크 전송, 개인정보처리시스템의 접근권한 부여 등 개인정보의 이전 또는 공동 이용하는 모든 행위를 말한다.

2.3 **목적 외 이용** : 개인정보처리자가 당초의 수집목적을 벗어나 다른 목적으로 개인정보를 이용하는 것을 말한다. 같은 개인정보처리자 내에서 당초 수집목적과 다른 목적으로 이용하기 위해 서로 다른 부서간에 개인정보를 제공하는 것도 목적 외 이용에 해당된다.

2.4 **목적 외 제3자 제공** : 개인정보처리자가 당초의 수집목적을 벗어나 다른 목적으로 이용하기 위하여 제3자에게 개인정보를 제공하는 것을 말한다.

3. 개인정보의 목적 외 이용·제공 기준

3.1 **원칙적으로 개인정보의 목적 외 이용 및 제3자 제공 금지**

- 정보주체에게 이용·제공의 목적을 고지하고 동의를 받은 범위 또는 법령에 의하여 이용·제공이 허용된 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 안 됨

< **개인정보보호법 제18조 제1항** >
개인정보처리자는 개인정보를 제15조(개인정보의 수집·이용) 제1항에 따른 범위를 초과하여 이용하거나 제17조(개인정보의 제공) 제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

3.2 예외적으로 아래의 사유에 해당하는 경우 목적 외 이용·제공 가능

단, 정보주체나 제3자의 이익을 부당하게 침해할 우려가 없는 경우에 한함

1) 정보주체로부터 **별도의 동의**를 받은 경우
2) **다른 법률에 특별한 규정**이 있는 경우
3) 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4) 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5) 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6) 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7) 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8) 법원의 재판업무 수행을 위하여 필요한 경우
9) 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

< **개인정보보호법 제18조 제2항** >
제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

4. 개인정보의 목적 외 이용·제공 처리절차

적정성 검토	- 목적 외 이용·제공 가능 여부에 대한 법적 근거 검토 - 목적 외 이용·제공하는 개인정보 항목의 적정성 검토 ⇒ 목적 외 이용·제공 여부 및 범위 판단
⇩	
동의 절차 이행	- 법적 근거가 없는 경우 반드시 정보주체의 별도 동의 필요 - 법 제18조제3항에 따른 의무사항 반드시 준수
⇩	
목적 외 이용 · 제공	- 이용·제공 처리기준 및 제공받는 자의 제한사항 - 목적 외 이용 및 제공 방법
⇩	
대장 기록 · 관리	- "개인정보의 목적 외 이용 및 제3자 제공" 대장 기록·관리
⇩	
주요 내용 공개	- 목적 외 이용 또는 제3자 제공한 날로부터 30일 이내에 관보 또는 인터넷에 게재 (인터넷의 경우 10일 이상 계속 게재)
⇩	
보호조치 요구	- 제3자에게 제공시 이용목적, 이용기간, 이용형태 등을 제한하거나 개인정보 안전성 확보를 위한 필요한 조치를 마련토록 문서로 요청
⇩	
조치결과 제출	- 안전성 확보 조치를 요청 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알림

4.1 목적 외 이용·제공의 적정성 검토

1) 문서접수

- 전자문서가 원칙이나 법원문서 등 불가피한 경우는 예외
- 필수 확인사항 : 법적 근거, 목적, 개인정보 항목, 이용기간

2) 법적 근거 검토

- 법 제18조 제2항에 해당하는 여부
- 개별법의 관련 규정 확인
  - 개별법에 "법령상 의무이행"과 같이 포괄적으로 규정되어 있거나, 시행령·시행규칙에만 규정이 있는 경우는 제공 불가
  - 단, 법률에 위임 근거가 있고 이에 따라 시행령·시행규칙에 관련 규정이 있는 경우 제공 가능
  - 다른 법률의 특별한 규정에 해당된다는 행정자치부의 질의회신 문서를 첨부한 경우 요청 목적 등을 확인 후 제공 가능

3) 개인정보 항목의 적정성 검토

- 道에서 수집한 개인정보 여부
  - 道에서 수집한 정보에 한하여 제공 가능
  - 다른 기관으로부터 제공받아 이용하는 정보는 제공 불가
    (단, 정보주체로부터 별도의 동의를 받았거나 다른 법률에 특별한 규정이 있는 경우는 제공 가능)
- 목적 외 이용·제공 목적에 부합하는 최소 항목 여부
  - 요청 목적과 부합하지 않거나 과도하다고 판단되는 경우 해당 항목을 제외하고 최소 범위로 제공
  - 개별법에서 항목을 열거하고 있는 경우 해당 항목에 한해 제공

개인정보의 목적 외 이용·제공 여부는 요청 기관(부서)의 개별법과 개인정보보호법 및 지침 등을 종합적으로 참조하여 판단하고, 정보주체 또는 제3자의 이익을 침해하지 않는 범위 내에서 최소한의 항목만 제공

4.2 정보주체의 동의절차 이행

1) 정보주체로부터 별도의 동의 이행

- 동의를 받아야 하는 시점, 절차 등에는 특별한 제한은 없으나 수집·이용에 대한 동의 항목과 목적 외 이용·제공 동의 항목을 별도로 구분하여 동의를 받아야 함
- 반드시 정보주체의 동의를 받아야 하므로 가족의 개인정보를 요청한 경우에 가족 개개인의 동의 필요

2) 동의 획득 시 고지사항 준수

- 법 제18조 제3항에 따른 필수 고지사항을 정보주체에게 알려야 하며, 필수 고지사항이 변경된 경우 이를 다시 알리고 동의를 받아야 함
- 목적 외 이용 시 필수 고지사항
  - 개인정보의 이용 목적
  - 이용하는 개인정보의 항목
  - 개인정보의 보유 및 이용기간
  - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

- 목적 외 제공 시 필수 고지사항
  · 개인정보를 제공 받는 자
  · 제공받는 자의 이용 목적, 제공하는 개인정보의 항목
  · 제공받는 자의 개인정보 보유 및 이용기간
  · 동의를 거부할 권리가 있다는 시실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

개인정보의 목적 외 이용·제공을 위한 **정보주체의 동의**는 법 제18조 제3항에 따른 의무사항을 준수해야 하는 **개인정보 보유기관**이 받아야 함.

4.3 목적 외 이용·제공

1) 이용·제공 처리기준 및 제한사항

- 목적 외 이용 계획, 제공, 결과, 개인정보 파기 등 목적 외 이용에 관한 사항은 전자문서 시행을 원칙으로 함
- 목적 외 제공시 전자문서 필수 기재 사항
  · 이용 목적, 이용 방법, 이용 기간, 이용 형태의 제한사항
  · 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치사항

< **회신문안 예시** >
- 본 자료는 개인의 사생활과 밀접한 관련이 있는 개인정보로 「개인정보보호법」 등 관련 법령에 맞게 이용·관리하시기 바랍니다.
- 본 자료는 요청 목적 외의 용도로 이용하거나, 정보주체의 동의 없이 다른 기관에 재제공하는 행위는 금지됩니다.
- 개인정보를 제공받은 목적이 달성된 후에는 반드시 완전 파기하는 등 「개인정보보호법」에 따라 안전성 확보를 위한 조치를 해주시기 바랍니다.
- 본 자료는 신고사항 등에 기초한 자료이므로 향후 변동될 수 있습니다.

- 개인정보 수령자의 인적사항을 반드시 확인하여 기록·관리
- 관련 업무 처리 후 PC에 개인정보 자료가 저장된 경우 지체 없이 삭제

2) 개인정보 제공 방법

- 전자문서 등 정보통신망을 이용하여 제공하는 경우
  · 개인정보를 엑셀 등 첨부파일 형태로 제공하되, 반드시 암호화 조치하여 송부하고 암호는 유선 등의 방법으로 별도 통보
  (문서 등 본분에 개인정보 및 비밀번호를 표기하여 제공 불가)

- 문서 출력물에 의한 제공하는 경우
  · 요청기관의 담당자 또는 직상급자에게 직접 전달
  · 우편을 이용하는 경우 배달증명으로 발송
- 보조기억매체를 이용하여 제공하는 경우
  · 보안USB 사용을 권장하며 제공되는 자료는 반드시 암호화 조치
  · 자료전달 후 반출된 보조기억매체에 저장된 자료는 즉시 삭제
  · 요청기관의 담당자 또는 직상급자에게 직접 전달
- 그 밖의 방법으로 제공이 필요한 경우 안전성 조치 등에 대해 개인정보보호담당자와 협의를 거쳐 제공

4.4 대장 기록·관리

1) 목적 외 이용·제공시에는 반드시 “개인정보의 목적 외 이용 및 제3자 제공 대장”에 기록·관리함

4.5 개인정보의 목적 외 이용·제공 공고

1) 공고방법 및 기간
   - 목적 외 이용하거나 제3자에게 제공한 날로부터 30일 이내에 경기도대표홈페이지 공지사항에 10일 이상 계속 게재

     ※ 소속기관의 경우 소속기관 홈페이지에 공고 가능
2) 필수 기재사항
   - 이용·제공 일자, 법적 근거, 제공 목적, 제공하는 개인정보의 항목

4.6 안전성 확보 조치

1) 목적 외 제3자 제공시 문서로 시행하여야 하며, 문서에 제공 목적 외 이용 금지, 이용목적 달성 후 폐기, 사후관리 실태 확인 등의 안전성 확보 조치 문구를 표기하여 시행
2) 제공받은 기관의 개인정보 안전성 확보 조치 결과 문서 접수

별첨1 **관련 서식**

개인정보의 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="3">[ ] 목적외 이용 [ ] 제3자 제공</td></tr>
<tr><td>목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td></td><td rowspan="3">담당자</td><td>소 속
성 명
전화번호</td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td>성 명
소 속
전화번호</td></tr>
<tr><td>이용하거나 제공한 날짜,
주기 또는 기간</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한 형태</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공의 법적
근거</td><td colspan="3"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="3"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라
제한을 하거나 필요한
조치를 마련할 것을
요청한 경우에는 그 내용</td><td colspan="3"></td></tr>
</table>

별첨2 개인정보의 단계별 규제 수준 비교

구 분	수집·이용 및 제공기준	목적외 이용·제공 기준
공통기준		· 정보주체 또는 제3자의 이익을 부당하게 침해하지 않는 범위 안에서만 목적외 이용·제공이 가능함
동의	· 정보주체의 동의를 받은 경우 ⇒ 수집·이용 및 제공 가능	· 정보주체로부터 별도의 동의를 받은 경우 (모든 개인정보처리자)
법률규정	· 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 다른 법률에 특별한 규정이 있는 경우 (모든 개인정보처리자)
공공기관 소관업무 수행	· 공공기관이 소관 업무 수행을 위하여 불가피한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 개인정보를 목적 외로 이용하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의를 거친 경우 (공공기관만 적용)
계약이행	· 계약의 이행을 위해 불가피하게 수반되는 경우 ⇒ 수집 및 해당 목적범위 안에서 이용 가능 (제공 불가)	
정보주체 또는 제3자의 이익	· 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 (모든 개인정보처리자)
개인정보처리자의 이익	· 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우 ⇒ 수집 및 해당 목적범위 안에서 이용 가능 (제공 불가)	
통계·학술연구 목적		· 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우
국제협정이행		· 조약 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 (공공기관만 적용)
범죄수사 등		· 범죄의 수사와 공소제기 및 유지를 위하여 필요한 경우 (공공기관만 적용)
재판		· 법원의 재판업무 수행을 위하여 필요한 경우 (공공기관만 적용)
형·감호 집행		· 형 및 감호의 집행을 위하여 필요한 경우 (공공기관만 적용)

별첨3 관련 법령 발췌

□ 개인정보보호법

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자

2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정자치부령으로 정하는 바에 따라 관

보 또는 인터넷 홈페이지 등에 게재하여야 한다.

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

경기도 개인정보 유출 대응 매뉴얼

경 기 도
(기획조정실)

개 정 이 력

[개인정보 유출 대응 매뉴얼]

개정번호	일 자	개 정 내 용	비고
1	2013.01.24.	매뉴얼 제정	
2	2013.10.28.	매뉴얼 1차 개정	
3	2015.06.23	매뉴얼 2차 개정	

경기도 개인정보 유출 대응 매뉴얼

1. 적용범위

1.1 본 매뉴얼은 경기도 정보보호관리체계 범위 안의 소속직원 및 정보시스템을 그 대상으로 한다.

1.2 본 매뉴얼은 개인정보의 유출시 대응절차를 규정하며, 개인정보의 유출이 불법적인 침해로 발생된 사고의 경우에는 본 매뉴얼의 이행과 함께 “경기도 사이버침해 대응운영 절차서”에 따른 절차를 이행하여야 한다.

2. 목적

본 매뉴얼은 개인정보 유출 발생시 「개인정보보호법」에 따른 법적 요건을 준수하고, 개인정보 유출에 따른 피해 확산 및 추가 유출을 효과적으로 방지하는데 그 목적이 있다.

3. 용어의 정의

3.1 개인정보 : 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

3.2 개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

3.3 개인정보 보호책임자 : 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.

3.4 개인정보 보호담당자 : 개인정보 보호책임자의 업무를 보조하기 위하여 총괄부서에 개인정보 보호 업무만을 전담하는 자를 말한다.

3.5 총괄부서 : 도 개인정보 보호업무를 주관하는 부서를 말한다.

3.6 분야별 책임자 : 개인정보(파일)를 보유한 부서장을 말한다.

3.7 개인정보취급자 : 분야별 책임자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자를 말한다.

3.8 개인정보 침해 : 법적 근거, 규정 또는 본인 동의에 의하지 않고 이루어지는 개인정보의 수집, 저장, 이용 및 제공, 파기행위 일체를 말하며, 개인정보 침해유형에는 개인정보 유출과 노출 등이 있다.

3.9 개인정보 유출 : 법령이나 개인정보처리자의 자유로운 의사에 따르지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

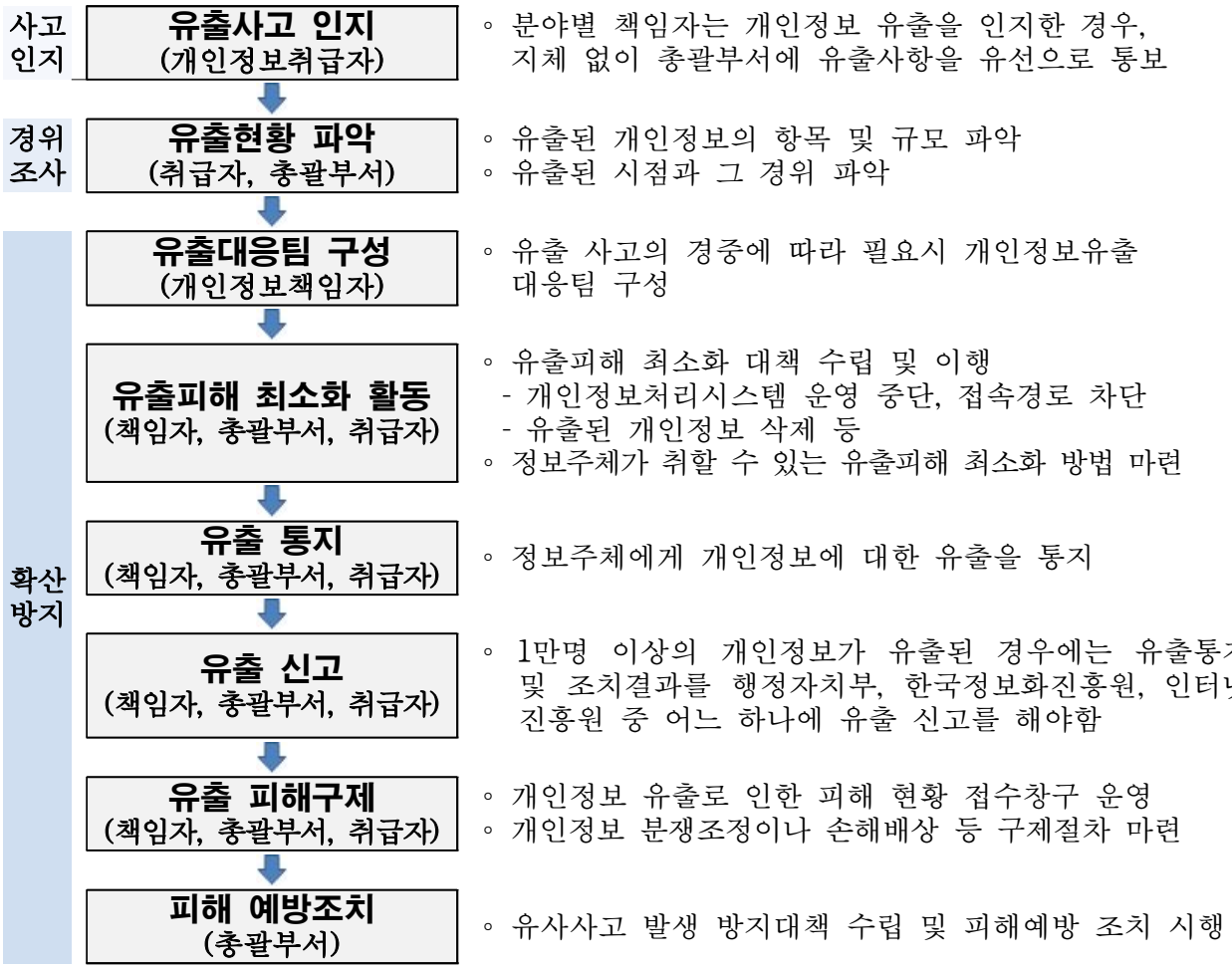
1) 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2) 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3) 개인정보처리자의 고의 또는 과실로 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4) 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

3.10 개인정보 노출 : 일반 인터넷 이용자가 해킹 등 특별한 방법을 이용하지 않고 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷에 방치된 것으로 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1) 개인정보취급자 및 민원인의 부주의로 홈페이지 게시물 및 게시판의 첨부파일(엑셀, 한글, PDF 등)에 포함된 개인정보 노출
2) 홈페이지의 공개 소스코드 또는 URL에 개인정보가 포함되어 노출된 경우
3) 구글 등 포털의 검색로봇 수집에 따른 개인정보 노출

4. 개인정보 유출 대응

4.1 유출대응 절차



4.2 유출사고 인지 및 보고

1) 분야별 책임자는 개인정보 유출을 인지한 경우, 지체 없이 총괄부서에 유출사항을 유선으로 통보하고, 개략적인 “개인정보 유출신고서”를 작성·제출한다.

2) 개인정보 유출사항을 통보받은 총괄부서는 유출된 개인정보의 항목 및 규모를 확인하고, “개인정보 유출신고서”를 통하여 개인정보 보호책임자에게 유출사항을 보고한다.

3) 개인정보 유출 관련 언론 대응 및 대외기관과의 협력 등은 총괄부서에서 총괄 수행한다.

4.3 개인정보 유출대응팀 구성 및 임무

1) 개인정보 보호책임자는 개인정보 유출 대응을 위해 개인정보 유출대응팀을 구성·운영할 수 있고, 구성 시기는 개인정보 보호책임자가 팀을 구성하도록 승인한 날부터 종료하도록 지시한

날까지로 한다.

2) 개인정보유출대응팀은 개인정보 보호책임자가 총괄팀장이 되고, 총괄부서의 장이 대책반장이 된다.

3) 대책반장의 임무는 다음 각 호와 같다.

가) 유출사고 범위와 유형에 따라 필요한 분야별 대응팀 구성·운영

나) 분야별 대응팀 업무와 팀장 지정을 포함한 개인정보유출대응팀 운영계획을 수립하여 관련 부서에 통보

다) 개인정보유출대응팀 구성 종료 시 개인정보유출대응팀 종합 활동보고서를 작성하여 총괄팀장에게 보고

4) 분야별 대응팀은 조사분석팀, 사고대응팀, 사고부서대응팀 등으로 구성·운영하고 필요시 외부전문가 등을 포함할 수 있으며, 대응팀별 임무는 다음 각호와 같다. 다만, 개인정보의 유출이 개인정보 취급자의 고의적인 행위에 기인한 경우, 해당 개인정보 취급자는 대응팀에 포함될 수 없으며, 해당 부서의 참여도 최소화한다.

가) 조사분석팀 : 개인정보 유출 규모, 시점·경위, 원인 등에 대한 분석 업무를 담당

나) 사고대응팀 : 개인정보 유출 피해 최소화 활동, 유출 통지, 유출 신고 등의 업무를 담당

다) 사고부서대응팀 : 조사분석팀과 사고대응팀에 관계 물품·서류 등 자료 제출 등 협조

라) 분야별 대응팀의 팀장이 속한 부서장은 자체 세부운영계획과 분야별 대응팀의 팀원을 지정하여 대책반장에게 통보

마) 하루 1회 “개인정보유출 대응활동 보고서”를 작성하여 대책반장에게 보고하고, 대책반장은 이를 검토·보완하여 총괄팀장에게 일단위로 보고

5) 개인정보의 유출이 불법적인 침해에서 비롯된 경우에는 개인정보유출대응팀을 사이버침해대응센터와 통합 운영한다.

4.4 개인정보 유출 통지

1) 유출 통지 항목

가) 통지대상 개인정보는 아래 서식과 같이 의무통지 대상정보와 선택통지 대상정보로 구분하며, 선택통지 대상정보에 대한 통지 여부는 개인정보 보호책임자와 분야별 책임자가 결정한다.

통지대상	구 분	항 목
의무통지	고유식별정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
	민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력자료 정보
	금융정보	계좌정보(계좌번호·비밀번호), 신용카드정보(카드번호·비밀번호), 신용등급 등
	계정정보	아이디·비밀번호
선택통지	의무통지 이외 사항	습관, 취미, 학력, 훈련 정보 등

나) 통지대상 개인정보는 유출 건수와는 무관하게 이루어지며, 단 1건의 개인정보가 유출되었더라도 해당 정보주체에게 그 사실을 통지해야 한다.

다) 통지주체는 경기도가 되며, 통지행위는 개인정보 보호책임자의 협조·지시를 받아 분야별 책임자가 수행하고, 이를 “개인정보 유출신고서”에 포함하여 개인정보 보호책임자에게 보고한다.

2) 통지내용

가) 유출된 개인정보의 항목

나) 유출된 시점과 그 경위

다) 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

라) 개인정보처리자의 대응조치 및 피해 구제절차

마) 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

3) 통지시기

가) 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 통지하여야 한다. 이 때 개인정보 유출 시점과 확인시점의 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

나) 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보 삭제 등의 긴급한 조치가 필요한 경우에는 그 조치를 한 후에 지체 없이 정보주체에게 통지한다.

다) 개인정보의 유출을 알게 된 때 또는 유출사실을 알고 긴급한

조치를 취한 후에도 유출된 개인정보의 항목, 유출 시점 및 그 경위의 구체적인 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 먼저 통지하고, 추후 확인된 사항을 추가로 통지한다.

4) 통지방법

가) 전자우편, 전화 및 문자전송, 서면 등의 방법을 통하여 정보주체에게 개별적으로 통지한다.

나) 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 상기 통지내용을 경기도 홈페이지(또는 개인정보 유출 발생 시스템)에도 7일 이상 게시한다.

4.5 개인정보 유출 신고

1) 신고대상 : 유출된 개인정보의 정보주체 수가 1만명 이상인 경우에는 행정자치부, 한국정보화진흥원, 한국인터넷진흥원 중 어느 하나에 개인정보 유출 신고를 하여야 한다.

2) 신고시기 : 유출사실을 알게 된 때 지체 없이 하여야 하며, 정보주체에 대한 통지 및 조치결과 등을 “개인정보 유출신고서”를 통하여 신고한다.

3) 신고연기 : 시간적 여유가 없거나 특별한 사정이 있는 경우에는 전화를 통하여 먼저 신고한 후, 나중에 “개인정보 유출신고서”를 제출할 수 있다.

4) 신고내용 : 기관명, 통지여부, 유출된 개인정보 항목·규모, 유출 시점·경위, 유출피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서, 담당자 및 연락처 등

5) 신고방법 : 전자우편, 팩스, 인터넷사이트를 통해 유출사고 신고 및 신고서를 제출한다.

신고기관	행정자치부	한국인터넷진흥원	한국정보화진흥원
전화번호	02-2100-3489	118	02-2131-0111
팩스번호	02-2100-3490	02-405-5229	-
전자우편	118@kisa.or.kr		
인터넷사이트	www.privacy.go.kr		

4.6 비상연락체계

신속하고 적절하게 피해 확산을 방지하고 피해를 복구하기 위하여 비상연락체계를 유지한다.

구 분		역 할	연 락 처
대내	기획조정실장	개인정보 보호책임자	031-8008-2100
	정보화기획관	정보화업무 담당 국장	031-8008-2300
	정보통신보안담당관	총괄부서의 장	031-8008-3880
	정보보안정책팀장	정보보안정책 총괄	031-8008-2925
	개인정보 보호담당자	개인정보 보호 업무 전담	031-8008-2909
	정보자원관리팀장	시스템운영업무 총괄	031-8008-2921
	사이버침해대응센터	사이버침해대응 업무 지원	031-8008-4114
대외	국가사이버안전센터	공공기관 보안사고 접수 및 처리	국번없이 111
	한국지역정보개발원	시도 보안사고 접수 및 대응지원	02-3279-3460
	한국인터넷진흥원	민간기관 보안사고 접수 및 대응지원	국번없이 118
	유지보수업체	방화벽, IPS 등 장비지원	031-8008-2943

5. 개인정보 침해 대응 및 피해구제

5.1 개인정보 침해신고 접수

1) 개인정보 침해신고 접수는 경기도 홈페이지를 통한 접수와 외부기관(행정자치부, 한국정보화진흥원, 한국인터넷진흥원)을 통한 접수로 구분된다.
2) 경기도 홈페이지를 통한 접수는 총괄부서에서 수행한다.
3) 외부기관을 통한 접수는 총괄부서에서 외부기관과의 협조를 통해 수행한다.

5.2 개인정보 침해신고 대응

1) 총괄부서는 개인정보 침해신고가 접수되면 지체 없이 관련부서(개인정보 처리부서)를 조사하여 신고내용의 사실관계를 확인하고, 확인된 침해내용에 따라 적정 조치를 수행한 후 그 결과를 개인정보침해 신고자에게 통보한다.
2) 개인정보 침해 내용이 “3.9 개인정보 유출”에 해당되거나 “3.10 개인정보 노출”로 인하여 개인정보 유출이 발생한 경우에는 “4. 개인정보 유출 대응”에 따른 대응 활동을 이행한다.
※ 개인정보 노출은 수시 모니터링을 통하여 즉시 조치 수행

5.3 피해구제

1) 정보주체에게 개인정보 피해구제 상담을 위하여 개인정보 분쟁조정 위원회 및 감독기관을 통한 구제절차를 안내한다.

구 분	내 용
신청내용	◦ 개인정보 처리와 관련한 당사자 간의 분쟁 사항 등
신청방법	◦ 개인정보피해로 인한 분쟁조정은 웹사이트, 우편, 팩스, 방문 등을 통해 신청인이 직접 또는 대리로 신청 할 수 있음 ◦ 개인정보침해 관련 상담 또는 신고사건 처리과정에서 신청 ※ 개인정보 분쟁조정 위원회(전화 118, 웹사이트 http://privacy.kisa.or.kr)
효 력	◦ 개인정보 분쟁조정위원회의 조정 결정에 대해 신청인과 상대방이 이를 수락하여 조정이 성립된 경우에는 조정서를 작성하게 되며, 조정서의 내용은 개인정보보호법 제47조제5항의 규정에 따라 “재판상 화해” (민사소송법상 확정판결과 동일한 효력)가 부여됨

2) 개인정보 침해·유출사고로 정보주체가 손해를 입으면 경기도 개인정보 보호 조례에 따른다.

6. 관련 서식

6.1 개인정보 유출신고서

개인정보 유출신고서

기 관 명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성 명	부 서	직 위	연락처
	개인정보 보호책임자				
	분야별 책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

6.2 개인정보유출 대응활동 보고서

개인정보유출 대응활동 보고서

기 본 정 보			
부 서 명		대응팀명	
보 고 자		직급 및 직위	
근 무 자			
연 락 처	전화: H.P: Fax:		
활 동 내 용			
활동 일시	20 년 월 일	○○시 ~ ○○시	
활동 내용			
그 밖의 동향 보고			
그 밖의 동향보고			
※ 첨 부 :			

6.3 개인정보 유출 등 침해사고 관리대장

개인정보 유출 등 침해사고 관리대장

접수		신고개요	처리유형	종결일자	처리내용	비고
일시	신고자 유형					

* 신고자 유형은 직원/민원으로 구분
* 신고 개요는 신고 내용을 기록
* 처리유형은 사실 확인 중 / 상담 및 자료제공 / 타기관 이송 / 위법성 통보 수사 의뢰 / 법 위반 확인 불가 / 기타(징계위원회 회부)로 구분
* 종결일자는 개인정보유출 처리보고서 접수일을 기준으로 기록
* 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류증, 수시중) / 징계처분(파면, 해임, 정직, 감봉, 견책, 기타)로 구분

6.4 개인정보 유출 통지문 예시

표준 통지문안 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	**<제목>** - '유출 통지' 문구 포함
선생님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 선생님의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
선생님의 개인정보는 20○○년 ○월 ○일 ○○○시스템 장애 처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고, 유지보수업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 20○○년 ○월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 경기지방경찰청에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	**<유출된 시점과 경위>** - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - '귀하', '고객님' 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 등 총 6개입니다.	**<유출된 항목>** - 유출된 항목을 누락 없이 모두 나열 ※ '등'으로 생략하거나, '회사전화번호' 및 '집전화번호'를 합쳐서 '전화번호'로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	**<개인정보처리자의 대응조치>** - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근 통제, 시스템 모니터링 강화 등 조치한 내용 설명
경기지방경찰청이 발표한 수사 결과에 따르면 현재 해커는 검거되었고, 해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다.	**<피해 최소화를 위한 정보주체의 조치방법>** - 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내

따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나, 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다.	- 사건에 따라 다양한 피해를 추정하여 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구, 감독기관인 경기도 언제나민원실 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	**<개인정보처리자의 피해 구제절차>** - 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 - 보상이나 배상이 결정되지 않은 경우 계획과 절차를 안내 - 감독기관 등을 통한 구제절차도 안내
앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.	(개인정보처리자의 향후 대응계획) - 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 도민께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)
▸ 피해 등 접수 담당부서 : ○○○과 ▸ 피해 등 접수 전화번호 : 031-8008-XXXX ▸ 피해 등 접수 e-메일주소 : XXX@gg.go.kr	**<피해 등 신고 접수 담당부서 및 연락처>** - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센타 등 다른 부서를 지정한 경우 해당 부서를 안내
경기도청 직원 일동	(발신명의)

기타(개인정보처리방침, 위탁계약서 등)

개인정보 처리방침 작성시 유의사항

□ 개인정보 처리방침이란 ?

o 「**개인정보 처리방침**」이란 개인정보를 처리하고 있는 공공기관의 개인정보 처리기준 및 보호조치 등을 **문서화하여 공개**하는 것을 말함

o 개인정보 보호법에서는 공공기관 등 개인정보처리자로 하여금 개인정보 처리방침을 **수립·공개하도록 의무화**하고 있음 (법 제30조)

※ 개인정보 처리방침을 정하지 않거나 공개하지 않는 자는 **1천만원 이하 과태료**가 부과됨

□ 어떤 내용을 담아야 하는가?

o 개인정보 보호법 및 표준 개인정보 보호지침은 「**개인정보 처리방침**」에 포함되어야 하는 사항을 정하고 있음

<개인정보 처리방침 기재사항>

필수적 기재사항	임의적 기재사항
1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공에 관한 사항 (해당되는 경우에만 정함) 4. 개인정보처리의 위탁에 관한 사항 (해당되는 경우에만 정함) 5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항 6. 처리하는 개인정보의 항목 7. 개인정보의 파기에 관한 사항 8. 개인정보 보호책임자에 관한 사항 9. 개인정보 처리방침의 변경에 관한 사항 10. 개인정보의 안전성 확보조치에 관한 사항	1. 정보주체의 권익침해에 대한 구제방법 2. 개인정보의 열람청구를 접수·처리하는 부서 3. 영상정보처리기기 운영·관리에 관한 사항 (개인정보 보호법 제25조제7항에 따른 '영상정보처리기기 운영·관리방침'을 개인정보처리방침에 포함하여 정하는 경우)

※ **필수적 기재사항**이란 개인정보 보호법 제30조, 시행령 제31조, 표준 개인정보 보호지침 제37조에 따라 「개인정보 처리방침」에 반드시 모두 포함해야 하는 사항임

※ **임의적 기재사항**이란 「개인정보 처리방침」에 포함시킬지 여부를 공공기관 스스로가 개인정보 처리현황을 고려하여 자율적으로 정할 수 있는 사항임

□ 어떻게 공개해야 하는가?

o **공공기관의 인터넷 홈페이지**에 지속적으로 게재해야 함

※ 반드시 "개인정보 처리방침"이라는 명칭을 사용하고, 글자크기·색상 등을 활용하여 다른 고지사항(이용약관, 저작권 안내 등)과 구분하여 정보주체가 쉽게 확인하도록 해야 함

o 인터넷 홈페이지에 게재할 수 없는 경우 **아래 방법**으로 공개해야 함

1) 공공기관 사무소 등의 보기쉬운 장소에 게시 2) 간행물, 소식지, 홍보지, 청구서 등에 지속적 게재
3) 관보 또는 공공기관 사무소가 있는 지역을 주된 보급지역으로 하는 일반일간신문 등에 게재
4) 재화·용역 제공을 위해 공공기관과 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급

개인정보 처리방침 항목별 작성방법 및 예시

◇ 비고

개인정보 처리방침에 포함되는 각각의 항목에 대해서는 '제1조', 'I' , '1' 등과 같이 일련번호를 붙일수도 있으며, 또는 일련번호를 붙이지 않고 각각의 항목의 제목만을 정보주체가 잘 알아볼 수 있게 표시하여도 된다 (Bold 표시 등).

≪예시≫

- **제1조(개인정보의 처리목적)** OOO부는 ~
- **I. 개인정보의 처리목적** OOO부는~
- **개인정보의 처리목적** OOO부는~

※ 본 작성방법 및 예시문에서는 편의상 **'제0조'의 형식**으로 설명한다.

1 제목

≪작성방법≫

o 공공기관의 명칭을 포함하여 가장 상단에 기재함

≪예시≫

<공공기관명> 개인정보 처리방침

2 서문

≪작성방법≫

o 개인정보 처리방침(이하 '처리방침'으로 칭함)을 수립·공개하고자 하는 공공기관의 명칭을 주어로 하여 기재함

o 공공기관의 처리방침 수립·공개의 취지를 밝힘

≪예시≫

<공공기관명>은(는) 개인정보 보호법 제30조에 따라 정보주체의 개인정보를 보호하고 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 하기 위하여 다음과 같이 개인정보 처리지침을 수립·공개합니다.

3 개인정보의 처리 목적

≪작성방법≫

o 공공기관이 개인정보를 처리하기 위한 목적을 기재함

- 가능한 구체적이고 상세히 기재하되, 해당 사무의 개인정보 처리목적을 정보주체가 알기 쉽게 이해할 수 있을 정도로 표현하면 됨

※ "개인정보의 처리"란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말함, 즉 공공기관이 개인정보를 다루는 모든 행위를 의미함

o 개인정보 보호법 제32조에 따라 '개인정보파일'을 보유·운용하는 경우에는 해당 개인정보파일의 명칭, 처리목적, 항목, 보유기간을 기재함

- 원칙적으로 행정안전부에 개인정보파일을 등록한 사항을 전부 기재하되, 처리목적·항목 등의 분량이 너무 많아 기재가 곤란한 경우에는 정보주체가 알기 쉽게 이해할 수 있는 수준에서 요약하여 기재할 수 있음

※ 개인정보파일과 관련한 인터넷 홈페이지가 별도로 있는 경우에는 해당 홈페이지에서 해당 개인정보파일에 대한 개인정보 처리방침을 공개해야 하며, 대표 홈페이지에서는 제외

≪예시≫ 일반적인 처리목적 기재

제1조(개인정보의 처리목적) ① <공공기관명>은(는) 다음의 목적을 위하여 개인정보를 처리합니다. 처리하고 있는 개인정보는 다음의 목적 이외의 용도로는 이용되지 않으며, 이용 목적이 변경되는 경우에는 개인정보 보호법 제18조에 따라 별도의 동의를 받는 등 필요한 조치를 이행할 예정입니다.

1. 홈페이지 회원 가입 및 관리

회원 가입의사 확인, 회원제 서비스 제공에 따른 본인 식별·인증, 회원자격 유지·관리, 제한적 본인확인제 시행에 따른 본인확인, 서비스 부정이용 방지, 만 14세 미만 아동의 개인정보 처리시 법정대리인의 동의여부 확인, 각종 고지·통지 등을 목적으로 개인정보를 처리합니다.

2. 민원사무 처리

민원인의 신원 확인, 민원사항 확인, 사실조사를 위한 연락·통지, 처리결과 통보 등의 목적으로 개인정보를 처리합니다.

3. <해당 공공기관의 개인정보 처리업무>

<개인정보 처리업무에 따른 처리목적>으로 개인정보를 처리합니다.

≪예시≫ 공공기관의 개인정보파일에 따른 처리목적 기재

② OOO부가 개인정보 보호법 제32조에 따라 등록·공개하는 개인정보파일의 처리목적은 다음과 같습니다.

순번	개인정보파일의 명칭	운영근거 / 처리목적	개인정보파일에 기록되는 개인정보의 항목	보유기간
1	국가인재DB	국가공무원법 제19조의3 공직후보자 정보의 체계적 수집·관리	성명, 연령, 전문분야, 연락처, 현·전직 직위, 학력, 경력, 상훈 등	준영구
2	전자민원 신청이력	공공기록물 관리에 관한 법령 최근 3년간 전자민원 신청이력 정보제공	성명, 주민번호, 전화번호, 주소	3년
3	주민등록정보	주민등록법 제28조, 제30조 주민등록전산정보 관리, 주민등록증 발급 등	주민등록번호, 성명, 주소사항, 세대사항, 주민등록증 발급사항 등 (5개 분야 10개 사항 161개 세부항목)	영구
	OOO	OOO	OOO	

※ 좀더 상세한 <공공기관명>의 개인정보파일 등록사항 공개는 행정안전부 개인정보보호 종합지원 포털(www.privacy.go.kr) → 개인정보민원 → 개인정보 열람등 요구 → 개인정보파일 목록검색 메뉴를 활용해주시기 바랍니다.

4 개인정보의 처리 및 보유 기간

≪작성방법≫

o 공공기관은 정보주체로부터 동의받은 '보유·이용기간' 또는 법령에 따른 '보유·이용기간'에 따라 개인정보를 보유할 수 있다는 내용을 기재함

o 개인정보를 처리하는 사무에 따른 구체적인 처리·보유 기간을 기재함

o 관계 법령에 개인정보의 보유 기간에 대한 근거가 있는 경우에는 해당 법령명 및 조문번호, 법령에서 정한 보유기간을 기재함

o 개인정보 보호법 제32조에 따라 '개인정보파일'을 보유·운용하는 경우에는 '3. 개인정보의 처리목적'에서 개인정보파일의 보유기간을 기재한 것으로 갈음함

≪예시≫

제2조(개인정보의 처리 및 보유기간) ① <공공기관명>은(는) 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보를 수집시에 동의받은 개인정보 보유·이용기간 내에서 개인정보를 처리·보유합니다.

② 각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.

1. 홈페이지 회원 가입 및 관리 : 공공기관 홈페이지 탈퇴시까지
   다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지
   1) 관계 법령 위반에 따른 수사·조사 등이 진행중인 경우에는 해당 수사·조사 종료시까지
   2) 홈페이지 이용에 따른 채권·채무관계 잔존시에는 해당 채권·채무관계 정산시까지
   3) <예외 사유> 시에는 <보유기간> 까지
2. 민원사무 처리 : 민원처리 종료 후 3년
3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」시행령 제29조에 따른 본인확인정보 보관 : 게시판에 정보 게시가 종료된 후 6개월
4. 「OO에 관한 법률」제0조에 따른 개인정보 처리·보유 : 00년
5. <개인정보 처리업무> : <보유기간>

5 개인정보의 제3자 제공에 관한 사항 (해당되는 경우에만 정함)

≪작성방법≫

o 공공기관이 개인정보를 제3자에게 제공하는 경우에는 그에 관한 사항을 기재하고, 만일 제3자 제공이 없을 경우에는 본 항목은 기재하지 않음

※ "개인정보의 제3자 제공"이란 공공기관이 처리하고 있는 개인정보를 공공기관 외의 제3자에게 제공하거나 공유하는 행위를 말함(법 제17조)
※ 개인정보처리업무의 취급을 위탁받은 자(수탁자), 영업을 양수하는 자는 '제3자'에서 제외됨

o 공공기관은 정보주체의 동의를 받거나 법률의 규정 등 개인정보 보호법이 허용한 경우 이외에는 개인정보를 제3자에게 제공하지 않는다는 원칙을 기재함

o 현재 개인정보의 제3자 제공이 이루어지고 있는 경우에는 1) 개인정보를 제공받는 자(제3자), 2) 제3자의 이용목적, 3) 제공하는 개인정보 항목, 4) 제공받는 자의 보유·이용기간을 각각 기재함

o 개인정보의 제3자 제공이 다수에게 이루어지는 경우에는 각각의 제3자에 대해 기재함

≪예시≫

제3조(개인정보의 제3자 제공) ① <공공기관명>은(는) 정보주체의 동의, 법률의 특별한 규정 등 개인정보 보호법 제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.

② <공공기관명>은(는) 다음과 같이 개인정보를 제3자에게 제공하고 있습니다.

<개인정보를 제3자에게 제공하는 사무명>
- 개인정보를 제공받는 자 : <제공받는 자의 법인명 또는 명칭>
- 제공받는 자의 개인정보 이용목적 : <구체적 이용목적>
- 제공하는 개인정보 항목 : <각 항목>
- 제공받는 자의 보유·이용기간 : <OO시까지> 또는 <0년>

6 개인정보처리의 위탁에 관한 사항 (해당되는 경우에만 정함)

≪작성방법≫

o 공공기관이 개인정보 처리업무를 위탁하고 있는 경우에는 그에 관한 사항을 기재하고, 만일 개인정보처리의 위탁이 없을 경우에는 본 항목은 기재하지 않음

※ "개인정보 처리업무 위탁"이란 개인정보처리자(공공기관 등)의 목적을 위하여 개인정보를 외부의 제3자에게 맡겨 업무를 처리하는 것을 말함 (콜센터, A/S센터, 배송 등)

o 현재 개인정보 처리업무 위탁이 이루어지고 있는 경우에는 1) 위탁받은 자(수탁자), 2) 위탁하는 업무의 내용을 각각 기재함

o 수탁자에 대한 재위탁 제한에 관한 사항, 안전성 확보조치에 관한 사항, 관리·감독에 관한 사항을 각각 기재함

≪예시≫

제4조(개인정보처리의 위탁) ① <공공기관명> 은(는) 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

1. 전화 상담센터 운영
 - 위탁받는 자 (수탁자) : OOO 컨택센터
 - 위탁하는 업무의 내용 : 전화상담 응대, 부서 및 직원 안내 등

2. <위탁 사무명>
 - 위탁받는 자 (수탁자) : <수탁자의 법인명 또는 명칭>
 - 위탁하는 업무의 내용 : <수탁 사무명>

② <공공기관명> 은(는) 위탁계약 체결시 개인정보 보호법 제25조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적·관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다.

③ 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

7 정보주체의 권리·의무 및 행사방법

≪작성방법≫

o 해당 공공기관에 대해 정보주체가 개인정보 보호와 관련하여 지니는 권리·의무를 기재

o 해당 공공기관에 대해 정보주체가 지니는 개인정보 열람, 정정·삭제, 처리정지 등 행사방법, 행사절차 등을 구체적으로 기재

- 예를 들어 인터넷 홈페이지를 운영하고 있는 경우에는 인터넷 홈페이지를 통한 열람, 정정·삭제 등의 기능 구현을 상세히 설명

※ '회원정보 조회/변경' 기능, '가입해지/회원탈퇴/동의철회' 기능 등의 이용방법을 상세히 설명

≪예시≫

제5조(정보주체의 권리·의무 및 행사방법) ① 정보주체는 <공공기관명>에 대해 언제든지 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다.

1. 개인정보 열람요구
2. 오류 등이 있을 경우 정정 요구
3. 삭제요구
4. 처리정지 요구

② 제1항에 따른 권리 행사는 <공공기관명>에 대해 개인정보 보호법 시행규칙 별지 제8호 서식에 따라 서면, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며 <공공기관명>은(는) 이에 대해 지체없이 조치하겠습니다.

③ 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 <공공기관명>은(는) 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않습니다.

④ 제1항에 따른 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수 있습니다. 이 경우 개인정보 보호법 시행규칙 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

8 처리하는 개인정보 항목

≪작성방법≫

o 해당 공공기관이 처리하고 있는 각각의 개인정보 항목을 기재함

o 수집목적에 필요한 최소한의 정보(필수항목)과 그 외의 정보(선택항목)을 구분하여 기재함

- 다만 필수항목만을 수집하고 있고 선택항목은 따로 두지 않는 경우에는 필수항목/선택항목을 구분하지 않아도 됨

o 현재 처리하고 있는 개인정보 항목은 원칙적으로 전부 기재하되, 해당 사무의 특성 등에 따라 그 분량이 많아 전부 기재가 곤란한 경우에는 정보주체가 알기 쉽게 이해할 수 있는 수준에서 간략히 표현할 수 있음

※ 각각의 개인정보 항목을 유형별·분야별로 묶어서 기재할 수 있음

o 해당 사무 처리과정이나 인터넷 서비스 제공 과정에서 자동으로 생성·수집되는 개인정보 항목이 있는 경우에는 해당 사무와 개인정보 항목을 명시

o 개인정보 보호법 제32조에 따라 '개인정보파일'을 보유·운용하는 경우에는 '3. 개인정보의 처리목적'에서 처리하는 개인정보 항목을 기재한 것으로 갈음함

≪예시≫

제6조(처리하는 개인정보 항목) <공공기관명> 은(는) 다음의 개인정보 항목을 처리하고 있습니다.

1. 홈페이지 회원 가입 및 관리
   · 필수항목 : 성명, 생년월일, 아이디, 비밀번호, 주소, 전화번호, 성별, 이메일 주소, 아이핀번호
   · 선택항목 : 결혼여부, 관심분야

2. 민원사무 처리
   · 필수항목 : 성명, 주민등록번호, 전화번호, 주소
   · 선택항목 : 이메일주소

3. <개인정보 처리업무>
   · 필수항목 : <처리항목>
   · 선택항목 : <처리항목>

4. <개인정보 처리업무> (필수항목만 수집하는 경우)
   · <처리항목>, <처리항목>,

5. 인터넷 서비스 이용과정에서 아래 개인정보 항목이 자동으로 생성되어 수집될 수 있습니다. (자동으로 생성·수집되는 개인정보항목이 있는 경우)
   · IP주소, 쿠키, MAC주소, 서비스 이용기록, 방문기록, 불량 이용기록 등

9 개인정보 파기에 관한 사항

≪작성방법≫

o 해당 공공기관에서 처리하고 있는 개인정보가 불필요하게 되었을 경우 지체 없이 파기한다는 내용을 기재함

o 다른 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 보존을 명시하고 있는 해당 법령명 및 조문을 구체적으로 기재함

o 파기의 절차, 방법 등에 관한 세부적인 내용을 기재함

≪예시≫

제7조(개인정보의 파기) ① <공공기관명> 은(는) 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기합니다.

② 정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보(또는 개인정보파일)을 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차

<공공기관명> 은(는) 파기하여야 하는 개인정보(또는 개인정보파일)에 대해 개인정보 파기계획을 수립하여 파기합니다. <공공기관명> 은(는) 파기 사유가 발생한 개인정보(또는 개인정보파일)을 선정하고, <공공기관명>의 개인정보 보호책임자의 승인을 받아 개인정보(또는 개인정보파일)을 파기합니다.

2. 파기방법

<공공기관명> 은(는) 전자적 파일 형태로 기록·저장된 개인정보는 기록을 재생할 수 없도록 파기하며, 종이 문서에 기록·저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

10 개인정보의 안전성 확보조치에 관한 사항

≪작성방법≫

o 해당 공공기관이 개인정보 보호법 제24조제2항, 제29조 및 시행령 제30조에 따라 시행중인 안전성 확보조치에 관한 사항을 기재함

o 안전성 확보조치는 가능한 자세히 기재하되, 해당 공공기관의 안전성 확보조치에 관한 상세한 기술적 내용들이 알려짐으로써 개인정보 침해위협이 증가할 수 있다고 판단되는 경우에는 그 수준을 조절하여 표현할 수 있음

≪예시≫

제8조(개인정보의 안전성 확보조치) ① <공공기관명> 은(는) 개인정보의 안전성 확보를 위해 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치 : 내부관리계획 수립·시행, 정기적 직원 교육 등
2. 기술적 조치 : 개인정보처리시스템 등의 접근권한 관리, 접근통제시스템 설치, 고유식별정보 등의 암호화, 보안프로그램 설치
3. 물리적 조치 : 전산실, 자료보관실 등의 접근통제

11 개인정보 보호책임자에 관한 사항

≪작성방법≫

o 해당 공공기관이 개인정보 보호법 제31조에 따라 지정한 개인정보 보호책임자를 게재함

※ 개인정보 보호책임자는 공공기관의 성격, 규모 등을 고려하여 복수로 지정할 수 있으며, 다만 공공기관의 전체 개인정보 보호를 총괄 책임지는 1인의 최고 책임자가 반드시 지정되어야 함

o 개인정보 보호책임자의 성명, 직책, 직급, 연락처(전화번호, 이메일주소 등)를 기재함

- 공공기관의 직급의 경우, 개인정보 보호법 시행령 제32조제2항에 따른 기관별 직급에 부합하여야 함

- 연락처의 경우, 반드시 개인정보 보호책임자의 직통 연락처를 기재할 필요는 없으며 정보주체의 개인정보 관련 문의 또는 고충처리 등이 원활히 처리될 수 있는 개인정보 보호책임자의 소속 부서 연락처 등을 기재하여도 무방함

o 개인정보 보호책임자 이외에도 공공기관의 필요에 따라 개인정보 보호 담당부서, 담당자 등을 기재하는 것도 바람직함

≪예시≫

제9조(개인정보 보호책임자) ① <공공기관명> 은(는) 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호책임자
성명 : OOO
직책 : OOO실장
직급 : 3급
연락처 : <전화번호>, <이메일>, <팩스번호>
※ 개인정보 보호 담당부서로 연결됩니다.

▶ 개인정보 보호 담당부서
부서명 : OOO
담당자 : OOO
연락처 : <전화번호>, <이메일>, <팩스번호>

② 정보주체께서는 <공공기관명> 의 서비스(또는 사업)을 이용하시면서 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의하실 수 있습니다. <공공기관명> 은(는) 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

12 개인정보 열람청구를 접수·처리하는 부서 (임의 기재사항)

≪작성방법≫

o 정보주체가 해당 공공기관에 대해 개인정보 열람청구를 신청할 수 있는 부서명을 기재

- '11. 개인정보 보호책임자에 관한 사항'의 '개인정보 보호 담당부서'에서 개인정보 열람청구 업무를 담당한다고 기재하는 것도 무방함

o 행정안전부의 '개인정보보호 종합지원 포털'을 통해 열람청구를 접수할 수 있음을 같이 기재

≪예시≫

제10조(개인정보 열람청구) ① 정보주체는 개인정보 보호법 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. <공공기관명>은(는) 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

▶ 개인정보 열람청구 접수·처리 부서
부서명 : OOO
담당자 : OOO
연락처 : <전화번호>, <이메일>, <팩스번호>

② 정보주체께서는 제1항의 열람청구 접수·처리부서 이외에, 행정안전부의 '개인정보보호 종합지원 포털' 웹사이트(www.privacy.go.kr)를 통하여서도 개인정보 열람청구를 하실 수 있습니다.

▶ 행정안전부 개인정보보호 종합지원 포털 → 개인정보 민원 → 개인정보 열람등 요구 (본인확인을 위하여 아이핀(I-PIN)이 있어야 함)

13 권익침해 구제방법 (임의 기재사항)

≪작성방법≫

o 정보주체가 개인정보침해에 대한 구제를 받을 수 있도록 하기 위하여 개인정보 보호법에 따른 전문기관(개인정보침해신고센터, 개인정보분쟁조정위원회), 수사기관 등을 안내함

o 다만 정보주체가 해당 공공기관에 문의하기도 전에 바로 전문기관, 수사기관 등에 바로 문의할 경우에는 오히려 원활한 피해구제가 어려우므로, 해당 기관에 대한 문의는 해당 공공기관에 대한 문의, 피해구제를 통해 해결이 되지 않을 경우에 2차적으로 하여야 한다는 내용을 반드시 안내함

≪예시≫

제11조(권익침해 구제방법) 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의하실 수 있습니다.

<아래의 기관은 <공공기관명> 과는 별개의 기관으로서, <공공기관명> 의 자체적인 개인정보 불만처리, 피해구제 결과에 만족하지 못하시거나 보다 자세한 도움이 필요하시면 문의하여 주시기 바랍니다>

▶ 개인정보 침해신고센터 (한국인터넷진흥원 운영)
- 소관업무 : 개인정보 침해사실 신고, 상담 신청
- 홈페이지 : privacy.kisa.or.kr
- 전화 : (국번없이) 118
- 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 개인정보 분쟁조정위원회 (한국인터넷진흥원 운영)
- 소관업무 : 개인정보 분쟁조정신청, 집단분쟁조정 (민사적 해결)
- 홈페이지 : privacy.kisa.or.kr
- 전화 : (국번없이) 118
- 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 대검찰청 사이버범죄수사단 : 02-3480-3573 (www.spo.go.kr)

▶ 경찰청 사이버테러대응센터 : 1566-0112 (www.netan.go.kr)

14 영상정보처리기기 운영·관리에 관한 사항

≪작성방법≫

o 본 항목은 개인정보 보호법 제25조제7항에 따라 공공기관이 마련하여야 하는 '영상정보처리기기 운영·관리 방침'을 본 개인정보 처리방침에 포함시키는 경우에 적용함

※ '영상정보처리기기 운영·관리 방침'은 원칙적으로 별도로 정하여야 하나, 표준 개인정보 보호지침 제40조제2항에 따라 개인정보 처리방침에 포함시켜 정할 수 있음

o 영상정보처리기기 운영·관리에 관한 아래의 사항을 포함하여 기재함

1) 영상정보처리기기 설치근거·목적
2) 설치 대수, 설치 위치, 촬영 범위
3) 관리책임자, 담당부서 및 영상정보에 대한 접근권한자
4) 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
5) 영상정보 확인 방법 및 장소
6) 정보주체의 영상정보 열람 등 요구에 대한 조치
7) 영상정보 보호를 위한 기술적·관리적·물리적 조치
8) 기타 영상정보처리기기 설치·운영·관리에 필요한 사항

≪예시≫

제12조(영상정보처리기기 설치·운영) ① <공공기관명> 은(는) 아래와 같이 영상정보처리기기를 설치·운영하고 있습니다.

1. 영상정보처리기기 설치근거·목적 : <공공기관명> 의 시설안전·화재예방
2. 설치 대수, 설치 위치, 촬영 범위 : 청사 로비·민원실 등 주요시설물을 촬영범위로 00대 설치
3. 관리책임자, 담당부서 및 영상정보에 대한 접근권한자 : OOO 과 OOO 과장
4. 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
   - 촬영시간 : 24시간 촬영
   - 보관기간 : 촬영시부터 30일
   - 보관장소 및 처리방법 : OOO과 영상정보처리기기 통제실에 보관·처리
5. 영상정보 확인 방법 및 장소 : 관리책임자에 요구 (OOO과)
6. 정보주체의 영상정보 열람 등 요구에 대한 조치 : 개인영상정보 열람·존재확인 청구서로 신청하여야 하며, 정보주체 자신이 촬영된 경우 또는 명백히 정보주체의 생명·신체·재산 이익을 위해 필요한 경우에 한해 열람을 허용함
7. 영상정보 보호를 위한 기술적·관리적·물리적 조치 : 내부관리계획 수립, 접근통제 및 접근권한 제한, 영상정보의 안전한 저장·전송기술 적용, 처리기록 보관 및 위·변조 방지조치, 보관시설 마련 및 잠금장치 설치 등

15 개인정보 처리방침 변경에 관한 사항

≪작성방법≫

o 개인정보 처리방침의 시행일자, 그간의 변경이력을 게재함

o 이전의 개인정보 처리방침이 있는 경우에는 정보주체가 이전 버전을 비교·열람할 수 있도록 하여야 함

※ 이전 버전 개인정보 처리방침의 적용기간 등을 게재하고, 클릭할 경우 해당 버전으로 연결되도록 하는 등의 방법 이용

≪예시≫

제13조(개인정보 처리방침 변경) ① 이 개인정보 처리방침은 20XX. X. X부터 적용됩니다.

② 이전의 개인정보 처리방침은 아래에서 확인하실 수 있습니다.

- 20XX. X. X ~ 20XX. X. X 적용 (클릭)
- 20XX. X. X ~ 20XX. X. X 적용 (클릭)

[붙임] 개인정보 처리방침(전체 작성 예시)

본 개인정보 처리방침 (전체 작성 예시)는 공공기관의 개인정보 처리방침 작성에 참고가 될 수 있도록 제공해드리는 것입니다. 이는 하나의 예시에 불과한 것으로서, 각 공공기관에서 실제로 개인정보 처리방침을 작성하실 경우에는 반드시 공공기관의 사업특성, 개인정보 처리현황에 맞게 수정/가감하여 작성하여야 함을 유의해 주시기 바랍니다.

OOO부 개인정보 처리방침

OOO부는 개인정보 보호법 제30조에 따라 정보주체의 개인정보를 보호하고 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 하기 위하여 다음과 같이 개인정보 처리지침을 수립·공개합니다.

제1조(개인정보의 처리목적) ① OOO부는 다음의 목적을 위하여 개인정보를 처리합니다. 처리하고 있는 개인정보는 다음의 목적 이외의 용도로는 이용되지 않으며, 이용 목적이 변경되는 경우에는 개인정보 보호법 제18조에 따라 별도의 동의를 받는 등 필요한 조치를 이행할 예정입니다.

1. 홈페이지 회원 가입 및 관리

   회원 가입의사 확인, 회원제 서비스 제공에 따른 본인 식별·인증, 회원자격 유지·관리, 제한적 본인확인제 시행에 따른 본인확인, 서비스 부정이용 방지, 만 14세 미만 아동의 개인정보 처리시 법정대리인의 동의여부 확인, 각종 고지·통지, 고충처리 등을 목적으로 개인정보를 처리합니다.

2. 민원사무 처리

   민원인의 신원 확인, 민원사항 확인, 사실조사를 위한 연락·통지, 처리결과 통보 등의 목적으로 개인정보를 처리합니다.

② OOO부가 개인정보 보호법 제32조에 따라 등록·공개하는 개인정보파일의 처리목적은 다음과 같습니다.

순번	개인정보파일의 명칭	운영근거 / 처리목적	개인정보파일에 기록되는 개인정보의 항목	보유기간
1	국가인재DB	국가공무원법 제19조의3 공직후보자 정보의 체계적 수집·관리	성명, 연령, 전문분야, 연락처, 현·전직 직위, 학력, 경력, 상훈 등	준영구
2	전자민원 신청이력	공공기록물 관리에 관한 법령 최근 3년간 전자민원 신청이력 정보제공	성명, 주민번호, 전화번호, 주소	3년
3	주민등록정보	주민등록법 제28조, 제30조 주민등록전산정보 관리, 주민등록증 발급 등	주민등록번호, 성명, 주소사항, 세대사항, 주민등록증 발급사항 등 (5개 분야 10개 사항 161개 세부항목)	영구

※ 기타 OOO부의 개인정보파일 등록사항 공개는 행정안전부 개인정보보호 종합지원 포털(www.privacy.go.kr) → 개인정보민원 → 개인정보열람등 요구 → 개인정보파일 목록검색 메뉴를 활용해주시기 바랍니다.

제2조(개인정보의 처리 및 보유기간) ① OOO부는 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보를 수집시에 동의받은 개인정보 보유·이용기간 내에서 개인정보를 처리·보유합니다.

② 각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.

1. 홈페이지 회원 가입 및 관리 : 공공기관 홈페이지 탈퇴시까지
   다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지
   1) 관계 법령 위반에 따른 수사·조사 등이 진행중인 경우에는 해당 수사·조사 종료시까지
   2) 홈페이지 이용에 따른 채권·채무관계 잔존시에는 해당 채권·채무관계 정산시까지
   3) <예외 사유> 시에는 <보유기간> 까지
2. 민원사무 처리 : 민원처리 종료 후 3년
3. 「OO에 관한 법률」 제0조에 따른 개인정보 처리·보유 : 00년

제3조(개인정보의 제3자 제공) ① OOO부는 정보주체의 개인정보를 제1조(개인정보의 처리 목적)에서 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등 개인정보 보호법 제17조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.

② OOO부는 다음과 같이 개인정보를 제3자에게 제공하고 있습니다.

- 개인정보를 제공받는 자 : <제공받는 자의 법인명 또는 명칭>
- 제공받는 자의 개인정보 이용목적 : <구체적 이용목적>
- 제공하는 개인정보 항목 : <각 항목>
- 제공받는 자의 보유·이용기간 : <OO시까지> 또는 <0년>

제4조(개인정보처리의 위탁) ① OOO부는 원활한 개인정보 업무처리를 위하여 다

음과 같이 개인정보 처리업무를 위탁하고 있습니다.

<전화 상담센터 운영>
- 위탁받는 자 (수탁자) : OOO 컨택센터
- 위탁하는 업무의 내용 : 전화상담 응대, 부서 및 직원 안내 등

② OOO부는 위탁계약 체결시 개인정보 보호법 제25조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적·관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다.

③ 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

제5조(정보주체의 권리·의무 및 행사방법) ① 정보주체는 OOO부에 대해 언제든지 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다.

1. 개인정보 열람요구
2. 오류 등이 있을 경우 정정 요구
3. 삭제요구
4. 처리정지 요구

② 제1항에 따른 권리 행사는 OOO부에 대해 서면, 전화, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며 OOO부는 이에 대해 지체없이 조치하겠습니다.

③ 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 OOO부는 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않습니다.

④ 제1항에 따른 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수 있습니다. 이 경우 개인정보 보호법 시행규칙 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

⑤ 정보주체는 개인정보 보호법 등 관계법령을 위반하여 OOO부가 처리하고 있는 정보주체 본인이나 타인의 개인정보 및 사생활을 침해하여서는 아니됩니다.

제6조(처리하는 개인정보 항목) OOO부는 다음의 개인정보 항목을 처리하고 있습니다.

1. 홈페이지 회원 가입 및 관리
   - 필수항목 : 성명, 생년월일, 아이디, 비밀번호, 주소, 전화번호, 성별, 이메일주소, 아이핀번호
   - 선택항목 : 결혼여부, 관심분야

2. 민원사무 처리
   · 필수항목 : 성명, 주민등록번호, 전화번호, 주소
   · 선택항목 : 이메일주소

3. 인터넷 서비스 이용과정에서 아래 개인정보 항목이 자동으로 생성되어 수집될 수 있습니다.
   · IP주소, 쿠키, MAC주소, 서비스 이용기록, 방문기록, 불량 이용기록 등

제7조(개인정보의 파기) ① OOO부는 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기합니다.

② 정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보(또는 개인정보파일)을 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차

OOO부는 파기하여야 하는 개인정보(또는 개인정보파일)에 대해 개인정보 파기 계획을 수립하여 파기합니다. OOO부는 파기 사유가 발생한 개인정보(또는 개인정보파일)을 선정하고, OOO부는 개인정보 보호책임자의 승인을 받아 개인정보(또는 개인정보파일)을 파기합니다.

2. 파기방법

OOO부는 전자적 파일 형태로 기록·저장된 개인정보는 기록을 재생할 수 없도록 로우레벨포멧(Low Level Format) 등의 방법을 이용하여 파기하며, 종이 문서에 기록·저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

제8조(개인정보의 안전성 확보조치) ① OOO부는 개인정보의 안전성 확보를 위해 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치 : 내부관리계획 수립·시행, 정기적 직원 교육 등
2. 기술적 조치 : 개인정보처리시스템 등의 접근권한 관리, 접근통제시스템 설치, 고유식별정보 등의 암호화, 보안프로그램 설치
3. 물리적 조치 : 전산실, 자료보관실 등의 접근통제

제9조(개인정보 보호책임자) ① OOO부는 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호책임자

성명 : OOO
직책 : OOO 실장
직급 : O급
연락처 : <전화번호>, <이메일>, <팩스번호>
※ 개인정보 보호 담당부서로 연결됩니다.

▶ 개인정보 보호 담당부서
부서명 : OOO
담당자 : OOO
연락처 : <전화번호>, <이메일>, <팩스번호>

② 정보주체께서는 OOO부의 서비스(또는 사업)을 이용하시면서 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의하실 수 있습니다. OOO부는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

제10조(개인정보 열람청구) ① 정보주체는 개인정보 보호법 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. OOO부는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

▶ 개인정보 열람청구 접수·처리 부서
부서명 : OOO
담당자 : OOO
연락처 : <전화번호>, <이메일>, <팩스번호>

② 정보주체께서는 제1항의 열람청구 접수·처리부서 이외에, 행정안전부의 '개인정보보호 종합지원 포털' 웹사이트(www.privacy.go.kr)를 통하여서도 개인정보 열람청구를 하실 수 있습니다.

▶ 행정안전부 개인정보보호 종합지원 포털 → 개인정보 민원 → 개인정보 열람 등 요구 (공공아이핀을 통한 실명인증 필요)

제11조(권익침해 구제방법) 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의하실 수 있습니다.

<아래의 기관은 OOO부와는 별개의 기관으로서, OOO부의 자체적인 개인정보 불만처리, 피해구제 결과에 만족하지 못하시거나 보다 자세한 도움이 필요하시면

문의하여 주시기 바랍니다>

▶ 개인정보 침해신고센터 (한국인터넷진흥원 운영)
- 소관업무 : 개인정보 침해사실 신고, 상담 신청
- 홈페이지 : privacy.kisa.or.kr
- 전화 : (국번없이) 118
- 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 개인정보 분쟁조정위원회 (한국인터넷진흥원 운영)
- 소관업무 : 개인정보 분쟁조정신청, 집단분쟁조정 (민사적 해결)
- 홈페이지 : privacy.kisa.or.kr
- 전화 : (국번없이) 118
- 주소 : (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 대검찰청 사이버범죄수사단 : 02-3480-3573 (www.spo.go.kr)

▶ 경찰청 사이버테러대응센터 : 1566-0112 (www.netan.go.kr)

제12조(영상정보처리기기 설치·운영) ① <공공기관명> 은(는) 아래와 같이 영상정보처리기기를 설치·운영하고 있습니다.

1. 영상정보처리기기 설치근거·목적 : <공공기관명> 의 시설안전·화재예방
2. 설치 대수, 설치 위치, 촬영 범위 : 청사 로비·민원실 등 주요시설물을 촬영범위로 00대 설치
3. 관리책임자, 담당부서 및 영상정보에 대한 접근권한자 : OOO 과 OOO 과장
4. 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
   - 촬영시간 : 24시간 촬영
   - 보관기간 : 촬영시부터 30일
   - 보관장소 및 처리방법 : OOO과 영상정보처리기기 통제실에 보관·처리
5. 영상정보 확인 방법 및 장소 : 관리책임자에 요구 (OOO과)
6. 정보주체의 영상정보 열람 등 요구에 대한 조치 : 개인영상정보 열람·존재확인 청구서로 신청하여야 하며, 정보주체 자신이 촬영된 경우 또는 명백히 정보주체의 생명·신체·재산 이익을 위해 필요한 경우에 한해 열람을 허용함
7. 영상정보 보호를 위한 기술적·관리적·물리적 조치 : 내부관리계획 수립, 접근통제 및 접근권한 제한, 영상정보의 안전한 저장·전송기술 적용, 처리기록 보관 및 위·변조 방지조치, 보관시설 마련 및 잠금장치 설치 등

제13조(개인정보 처리방침 변경) ① 이 개인정보 처리방침은 20XX. X. X부터 적용됩니다.

② 이전의 개인정보 처리방침은 아래에서 확인하실 수 있습니다.

- 20XX. X. X ~ 20XX. X. X 적용 (클릭)
- 20XX. X. X ~ 20XX. X. X 적용 (클릭)
- 20XX. X. X ~ 20XX. X. X 적용 (클릭)

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법, 동법 시행령 및 시행규칙, 「표준 개인정보 보호지침」(행정안전부 예규 제45호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다. ② "을"이 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 개인정보보호법 제29조, 동법 시행령 제30조 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

---

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체없이 “갑”에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

③ “갑”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 “을”을 교육할 수 있으며, “을”은 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “갑”은 “을”과 협의하여 시행한다.

제8조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 기타 “을”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “갑” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “갑”이 전부 또는 일부를 배상한 때에는 “갑”은 이를 “을”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “갑”과 “을”이 서명 또는 날인한 후 각 1부씩 보관한다.

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명 : (인)	성 명 : (인)

2) 「개인정보 안전성 확보조치 기준 고시」(행정안전부 고시 제2011-43호) 에 따라 개인정보처리자 및 취급자는 1년에 1회 이상 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

개인정보 유출 시 필수 조치요령 (법 제34조)

개인정보 유출 사고 발생 시 이것만은 꼭 조치하세요!

1

유출된 정보주체 개개인에게 지체 없이 통지

⇨ **개인정보보호법 제34조 제1항**

- 시한 : 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)
- 통지 항목 : ①유출된 개인정보의 항목, ②유출 시점과 및 그 경위, ③피해 최소화를 위한 정보주체의 조치방법, ④기관의 대응조치 및 피해구제 절차, ⑤피해 신고 접수 담당부서 및 연락처

* 개인정보보호법 제75조 제2항 제8호(**3천만 원 이하의 과태료**)
정보주체에게 같은 항 각 호의 사항을 알리지 아니한 자

2

피해 최소화를 위한 대책 마련 및 필요한 조치 실시

⇨ **개인정보보호법 제34조 제2항**

- 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치 이행
- 긴급조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

* 피해 최소화 대책을 마련하지 않거나 필요한 긴급 조치를 하지 않은 경우 : **시정명령**

3

1만 명 이상 유출된 경우 유출 통지 결과를 신고

⇨ **개인정보보호법 제34조 제3항**

- 1만명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 행정자치부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고

* 개인정보보호법 제75조 제2항 제9호(**3천만 원 이하의 과태료**)
조치결과를 신고하지 아니한 자 (행정자치부 또는 전문기관에 통지 결과 등을 신고하지 않은 경우)

4

1만 명 이상 유출된 경우에는 추가적으로 홈페이지에 공지

⇨ **개인정보보호법 시행령 40조 제3항**

- 1만명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

* 홈페이지 등에 공지하지 않거나 7일 미만 게재하는 경우 : **시정명령**

개인정보 유출 표준 통지문안

※ 부가설명 란에 **필수사항은 < >, 참고사항은 ( )**로 표기 하였음

※ 필수사항이 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

※ 아래 예시를 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

표준 통지문안 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	**<제목>** - '유출 통지' 문구 포함
고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 고객님의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
고객님의 개인정보는 2010년 3월 5일 회원관리시스템 장애 처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고, 유지보수업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 2010년 4월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 서울지방경찰청에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	**<유출된 시점과 경위>** - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - '귀하', '고객님' 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 등 총 6개입니다.	**<유출된 항목>** - 유출된 항목을 누락 없이 모두 나열 ※ '등'으로 생략하거나, '회사전화번호' 및 '집전화번호'를 합쳐서 '전화번호'로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	**<개인정보처리자의 대응조치>** - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근 통제, 시스템 모니터링 강화 등 조치한 내용 설명

서울지방경찰청이 발표한 수사 결과에 따르면 현재 해커는 검거되었고, 해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다. 따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나, 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다.	**<피해 최소화를 위한 정보주체의 조치방법>** - 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내 - 사건에 따라 다양한 피해를 추정하여 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구, 감독기관인 0000부 민원신고센터 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	**<개인정보처리자의 피해 구제절차>** - 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 - 보상이나 배상이 결정되지 않은 경우 계획과 절차를 안내 - 감독기관 등을 통한 구제절차도 안내
앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.	(개인정보처리자의 향후 대응계획) - 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 고객님께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)
▸ 피해 등 접수 담당부서 : 고객지원과 ▸ 피해 등 접수 전화번호 : 02-2345-6789, -9876 ▸ 피해 등 접수 e-메일주소 : abcd@efgh.co.kr	**<피해 등 신고 접수 담당부서 및 연락처>** - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센타 등 다른 부서를 지정한 경우 해당 부서를 안내
(주)하나둘업체 임직원 일동	(발신명의)

분야별 주민등록번호 처리기준 상담사례집

2015. 12.

행정자치부

KISA 한국인터넷진흥원

목 차

일러두기 5

주민등록번호 처리금지 원칙 6

제1장 기본 원칙 7

1. 주민등록번호 처리금지 원칙 도입 배경 8
2. 주민등록번호 처리금지 기본 원칙 9
3. '법령에서 구체적으로 정한 경우'의 의미 10
4. '정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익'의 의미 12
5. 법령상 근거없는 주민등록번호 파기조치 13
6. 주민등록번호 일부 정보[앞자리 + 뒷자리 첫째숫자] 사용 15
7. 주민등록번호 일부 정보[뒷자리 전체 또는 일부] 사용 17
8. 주민등록번호 처리금지 원칙 위반에 따른 벌칙 18

제2장 일상생활 사례 19

9. 홈페이지 회원 가입·관리를 위한 주민등록번호 수집 20
10. 법령상 주민등록번호 수집근거가 있는 업무처리를 위해 홈페이지 회원 가입 시 주민등록번호 수집 21
11. 멤버십 회원자격 확인, 포인트 관리 등을 위한 주민등록번호 처리 22
12. 콜센터 상담 시 본인확인을 위한 주민등록번호 이용 23
13. 건물·시설 출입관리를 위한 주민등록번호 처리 24
14. 주민등록번호가 기재된 신분증의 육안 확인 25
15. 위임장에 주민등록번호 기재 26
16. 법무·노무사건 위임 시 주민등록번호 처리 28
17. 현금영수증 처리를 위하여 주민등록번호 처리 29

제3장 공공 행정 사례 31

18. 특허출원 청구 시 주민등록번호 기재 32
19. 공공기관에 '다수인 관련 민원' 제기 시, 주민등록번호 기재 34
20. 훈장·포장, 정부 표창의 공적심사를 위한 주민등록번호 처리 35
21. 기초생활수급자, 장애인 등 사회적 배려대상자에 대한 공공요금 경감을 위한 주민등록번호 처리 37
22. 지자체 일자리사업 참여자의 주민등록번호 처리 39
23. 희귀난치성질환자 의료비지원사업 참여자의 주민등록번호 처리 40
24. 보육교사 교육 및 자격증 발급을 위한 주민등록번호 처리 41
25. 청소년 상담복지센터 내담자의 주민등록번호 처리 43

제4장 인사 · 노무 · 세무 사례 45

26. 기업의 직원 채용시 이력서 · 지원서 등에 주민등록번호 기재 46
27. 공무원 임용, 공공기관 채용 지원서에 주민등록번호 기재 47
28. 장애인 우선 채용을 위한 주민등록번호 수집 · 이용 48
29. 신원조사를 위한 주민등록번호 수집 · 이용 50
30. 채용시 성범죄자 확인을 위한 주민등록번호를 수집 · 이용 52
31. 직원 인사기록에 주민등록번호 보유 55
32. 퇴사한 직원의 주민등록번호 보관 57
33. 사용증명서(재직증명서, 경력증명서 등)에 주민등록번호 기재 60
34. 자문료 등 수당 지급을 위한 주민등록번호 처리 61
35. 기부금영수증 발급을 위한 주민등록번호 수집 · 이용 63

제5장 의료 · 보건 사례 65

36. 병원 진료 · 검사 예약 위한 주민등록번호 이용 66
37. 환자의 친족 · 대리인의 의료기록 열람 청구 시 주민등록번호 수집 · 이용 68
38. 헌혈자의 주민등록번호 수집 · 이용 71

목 차

제6장 금융 · 보험 · 상거래 사례 73

39. CMS(자금이체서비스) 이용을 위한 주민등록번호 처리 74
40. 수표 거래 시 주민등록번호 배서 75
41. 긴급한 금융업무 처리시 주민등록번호 이용 76
42. 단체보험 가입을 위한 주민등록번호 처리 78
43. 귀금속 거래 시 주민등록번호 수집 80
44. 해외구매대행 서비스 이용 시 주민등록번호 처리 81
45. 렌터카 서비스 계약 시 주민등록번호 수집 · 이용 83

제7장 교육기관 사례 85

46. 교육정보시스템(NEIS) 입력 위한 학부모 · 보호자의 주민등록번호 수집 · 이용 86
47. 대학 입학전형 위한 지원자 주민등록번호 수집 · 이용 88
48. 스쿨뱅킹 서비스를 위한 주민등록번호 수집 · 이용 90
49. 장학금 신청 · 심사 및 지급을 위한 주민등록번호 수집 · 이용 91
50. 저소득층 교육비 지원을 위한 주민등록번호 수집 · 이용 93
51. 대학교 증명서(재학·졸업 등) 발급 시 주민등록번호 기재 95
52. 학교발전기금 기탁자의 주민등록번호 수집 · 이용 96

제8장 기타 사례 99

53. 동호회 회원의 주민등록번호 수집 · 이용 100
54. 교회 교인명부에 주민등록번호 기재 101
55. 주택조합의 조합원 명부에 주민등록번호 기재 103

일러두기

본 사례집은「개인정보 보호법」개정으로
주민등록번호 처리 법정주의가 시행됨에 따라
일상생활 속 주민등록번호 처리의 허용 또는 금지에 관한
기준 제시를 목적으로 합니다.

또한 발간일('15. 12월) 현재의 법령 기준에 따라
서술되어 있으므로 향후 관련 법령의 제·개정에 따라 주민등록번호의
처리 허용여부가 달라질 수 있습니다. 따라서 본 사례집을 실무에
활용하시는 경우에는 관련 법령을 다시 한번 확인하시기 바랍니다.

주민등록번호 처리금지 원칙

1. 개요

• 주민등록번호 처리(수집 · 이용 · 제공 등) 원칙적 금지를 주요 내용으로 「개인정보 보호법」 개정 (공포 ’13.8.6., 시행 ’14.8.7.)

- ’14.8.7.부터 법령상 구체적 근거없이 불필요한 주민등록번호 처리 행위 엄격히 제한

※ 정보통신서비스제공자의 이용자 주민등록번호 수집 · 이용 금지 제도는 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에 따라 ’12. 8.18.부터 시행

2. 주요 내용

• ‘주민등록번호 처리 법정주의’(법 제24조의2 제1항) 신설

- 주민등록번호 처리를 원칙적으로 금지하고, 다음 사유에 해당하는 예외적인 경우에만 허용 (위반시 3천만원 이하 과태료 부과)

〈 주민번호 예외적 처리 허용 사유 〉

1. 법령(법률 · 시행령 · 시행규칙)에서 구체적으로 주민번호 처리를 요구 · 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우
3. 기타 주민번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

3. 적용 예시

• 정부 표창의 수여를 위한 공적조서에 주민등록번호 기재

- 정부 표창의 수여를 위한 공적조서에 「정부 표창 규정」 별지 제4호서식에 따라 “성명·주민등록번호” 등을 기재하도록 규정한 근거법령 有
  → 주민번호 처리 허용

• 기업의 직원 채용 시 지원서에 주민등록번호 기재

- 채용 진행 단계에서 입사지원자의 주민등록번호 수집 · 이용 허용하는 근거법령 無
  → 주민번호 처리 금지

제 1 장

기본 원칙

제 1 장 기본 원칙

01 주민등록번호 처리금지 원칙 도입 배경

Q **주민등록번호 처리금지 원칙은 어떤 이유에서 도입되었습니까?**

A 주민등록번호 유출 및 오남용을 효과적으로 방지하기 위해서는 주민등록번호의 수집 · 이용 등 제반 처리행위를 최소화하는 것이 가장 바람직하다는 인식에서 주민등록번호 처리금지 원칙이 도입되었습니다.

상세 설명

주민등록번호는 행정, 금융, 의료, 복지 등 사회 전 분야에서 개인 식별을 위한 기초자료로 널리 사용되고 있습니다. 특히 주민등록번호는 전자정부 고도화 등 우리나라의 ICT 환경 발전의 기초 인프라로 널리 사용되어 왔고, 편리하고 신속한 개인 식별을 가능하게 함으로써 사회적으로 많은 편익을 가져다 주는 것도 사실입니다.

그러나 최근 들어 주민등록번호 수집 · 이용이 반드시 필요하지 않음에도 불구하고 관행적으로 과다 수집 · 이용하는 빈도가 매우 높게 나타나고 있고, 특히 상당수의 민간사업자와 공공기관 등은 단순 본인확인 목적으로 주민등록번호를 수집하는 경우가 많은 것으로 나타났습니다 (2013 개인정보보호 실태조사, 개인정보보호위원회 · 안전행정부).

이렇게 과다하게 수집 · 이용되고 있는 주민등록번호는 다시 불법적으로 해킹 · 유출되는 사례가 많으며, 유출된 주민등록번호는 명의도용, 피싱 사기 등에 널리 악용되고 있어 개인뿐만 아니라 기업과 사회 전체의 문제로 부각되고 있습니다.

특히 우리나라의 주민등록번호는 유일성과 평생불변성을 지니고 있어 그 주민등록번호를 변경하는 것이 원칙적으로는 불가능합니다. 따라서 만약 주민등록번호가 유출된경우에는 다른 개인정보 항목에 비해 피해가 지속 · 확산되는 심각성이 있습니다. 또한 주민등록번호는 민간 및 공공의 각종 데이터베이스(DB)나 서비스에서 기준 검색값(Primary Key)으로 널리 활용되고 있어 유출시 심각성이 더 크다고 하겠습니다.

이에 따라 정부와 국회는 「개인정보 보호법」을 개정('13.8.6.)하여, 주민등록번호는 그 공익적 필요성이 인정되어 법령에 규정된 경우 등 예외적 사유를 제외하고는 원칙적으로 수집, 이용, 제공, 보관할 수 없도록 하는 원칙을 도입하게 되었습니다.

02 주민등록번호 처리금지 기본 원칙

Q **주민등록번호 처리금지 원칙의 주요 내용은 무엇입니까?**

A 모든 개인정보처리자는 원칙적으로 주민등록번호를 처리할 수 없습니다. 다만 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 등에만 예외적으로 주민등록번호를 처리할 수 있습니다.

상세 설명

민간 사업자, 공공기관 등 모든 개인정보처리자는 원칙적으로 주민등록번호를 처리할 수 없습니다. 즉 주민등록번호를 수집하여 이용하거나, 제3자에게 제공하거나, 저장·보유하는 행위 등이 모두 금지됩니다.

* '처리'란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말함 (개인정보 보호법 제2조제2호 참조)

다만 개인정보처리자는 다음의 사유에 해당하는 경우에는 예외적으로 주민등록번호를 처리할 수 있습니다 (개인정보 보호법 제24조의2제1항).

1) 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

2) 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

3) 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

기본적으로 '법령에서 주민등록번호 처리 요구 · 허용 근거'가 있어야만 주민등록번호의 수집 · 이용 등이 가능하다는 점에서 '주민번호 수집 법정주의'라고도 부르고 있습니다.

관련 법령

「개인정보 보호법」

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

03 '법령에서 구체적으로 정한 경우'의 의미

Q **'법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'란 어떤 의미입니까?**

A 법률, 시행령, 시행규칙 중 최소한 어느 하나에 개인정보처리자로 하여금 주민등록번호의 처리를 요구하거나 허용하도록 하는 구체적인 규정이 존재하는 것을 말합니다.

상세 설명

「개인정보 보호법」에서 지칭하는 '법령'이란 법률, 대통령령, 총리령, 부령을 의미합니다. 따라서 "법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우"라 함은 법률 또는 대통령령, 총리령, 부령에 개인정보처리자로 하여금 주민등록번호의 처리를 요구 · 허용하도록 하는 구체적인 근거 규정이 마련되어 있는 것을 의미합니다.

* '법령'이란 법률, 대통령령, 총리령 및 부령을 말함 (법제업무 운영규정 제2조 참조)

또한, 법령에 근거 규정이 있다는 의미는 법령 조문에 그 근거규정이 마련되어 있는 경우를 의미하지만, 그 외에 법령의 '별지 서식'에 주민등록번호의 기재 항목이 있거나, 법령에서 주민등록번호가 기재된 각종 공부(公簿)의 제출 · 첨부 등을 규정한 경우에도 법령 근거가 있는 것으로 봅니다(행정자치부, 주민등록번호 수집 금지 제도 가이드라인, 2014).

〈예 1〉 법령 조문에 주민등록번호의 처리 요구 · 허용 근거가 있는 경우

「의료법」 시행규칙
제14조(진료기록부 등의 기재 사항) ① 법 제22조제1항에 따라 진료기록부·조산기록부와 간호기록부(이하 "진료기록부등"이라 한다)에 기록해야 할 의료행위에 관한 사항과 의견은 다음 각 호와 같다.
1. 진료기록부
가. 진료를 받은 사람의 주소·성명·연락처·**주민등록번호** 등 인적사항 (이하 생략)

〈예 2〉 법령 별지 서식에 주민등록번호의 기재 항목이 있는 경우

■ 지방세법 시행규칙[별지 제37호서식] (앞쪽)

관 리 번 호	-	주민세(재산분) 신고서		
신고인 (납세자)	① 사업장명(상 호)			
	② 성 명(법 인 명)		③ 주민(법인)등록 번 호	
	④ 사업장(과세대상) 소 재 지		⑤ 사업자등록번호	
	⑥ 전 화 번 호		⑦ F A X 번 호	

〈예 3〉 주민등록번호가 기재된 공부(公簿)의 제출·첨부를 요구하는 경우

「국민건강보험법」 시행규칙
제2조(피부양자 자격의 인정기준 등) ④ 직장가입자가 피부양자 자격 취득 또는 상실 신고를 하거나 피부양자가 제3항제8호에 따른 자격 상실 신고를 하려면 별지 제1호서식의 피부양자 자격(취득·상실) 신고서에 다음 각 호의 서류(자격 취득 신고의 경우만 해당한다)를 첨부하여 공단에 제출하여야 한다. (이하 생략)

1. **가족관계등록부**의 증명서 1부(**주민등록표 등본**으로 해당 직장가입자와의 관계를 확인할 수 없는 경우만 해당한다) (이하 생략)

참고로, 각급 행정기관의 훈령 · 예규 · 고시 및 지방자치단체의 조례 · 규칙 등은 「개인정보 보호법」 제24조의2에서 규정하는 '법령'에 해당하지 않습니다. 따라서 이러한 행정규칙이나 지방자치단체의 조례 등에서 주민등록번호의 처리를 요구 · 허용한 규정이 있더라도 이는 법령에서 구체적으로 주민등록번호의 처리 요구 · 허용 근거를 둔 것에 해당하지 않음을 유의하여야 합니다.

또한, 법령에서 단순히 신원확인 또는 연령확인 등의 의무만을 규정하고 있다면 이 또한 주민등록번호 처리근거를 구체적으로 규정한 것에 해당하지 않습니다. 따라서 이 때에는 주민등록번호에 대한 구체적인 처리 근거를 법령에 신설하여야 합니다(행정자치부, 주민등록번호 수집 금지 제도 가이드라인, 2014).

04 '정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익'의 의미

Q **"정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 주민등록번호의 처리가 명백히 필요하다고 인정되는 경우"란 어떤 의미입니까?**

A 법령의 구체적인 근거가 없더라도 정보주체의 주민등록번호를 수집 · 이용 · 제공함으로써 정보주체의 급박한 생명, 신체, 재산 상의 위급상황을 벗어나는 것이 필요한 경우를 말합니다.

상세 설명

「개인정보 보호법」은 정보주체 또는 제3자의 급박한 생명, 신체, 재산상 이익을 위하여 필요하다고 인정되는 경우에는 정보주체의 동의 없이 개인정보를 수집 · 이용하거나 제3자에게 제공할 수 있도록 하고 있습니다 (「개인정보 보호법」제15조제1항제5호, 제17조제1항제2호 참조). 이는 정보주체의 생명권, 신체권, 재산권 등 헌법 상의 기본권적 가치를 급박하게 보호하기 위하여 필요한 경우에는 정보주체의 개인정보 자기결정권에 상대적으로 우선하여 이들 가치를 보호하고자 하는 입법적 취지로 볼 수 있습니다.

이러한 제도는 주민등록번호 처리금지 원칙에도 마찬가지로 적용되고 있습니다. 즉 정보주체나 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 주민등록번호의 수집 · 이용 등이 명백히 필요하다고 인정되는 경우에는 관련 법령에 주민등록번호 처리에 대한 구체적 근거 규정이 없더라도 주민등록번호의 수집 · 이용 등을 허용하고 있습니다(「개인정보 보호법 제24조의2제1항제2호).

다만 이는 단순히 정보주체의 생명, 신체, 재산상의 이익을 위한다는 이유만으로 바로 허용되는 것은 아닙니다. 우선 명백히 그 주민등록번호의 처리가 정보주체나 제3자의 생명, 신체, 재산상의 이익을 위한 것이어야 하며, 반드시 '급박성'이 인정되어야 합니다. 충분한 시간적인 여유가 있거나 다른 수단에 의해 생명, 신체, 재산상의 이익을 보호할 수 있다면 급박한 상태에 있다고 할 수 없습니다.

* '정보주체 또는 제3자의 생명, 신체, 재산상의 이익을 위한 개인정보 처리'의 의미에 대해 보다 상세한 내용은 행정자치부, 개인정보 보호법령 및 지침 · 고시 해설(2011) 참조.

05 법령상 근거없는 주민등록번호 파기조치

Q **그동안 업무상 필요에 의해 주민등록번호를 수집·보관하여 왔으나, 검토해 본 결과 '법령에 따른 구체적 처리근거'가 없습니다. 이런 경우에는 어떻게 해야 하나요?**

A 법령에 따른 구체적 처리근거가 없는 주민등록번호는 2016년 8월 6일 전에 파기 조치하여야 합니다.

상세 설명

「개인정보 보호법」개정 시행('13.8.6) 당시 주민등록번호를 처리하고 있는 개인정보처리자는 법령에 따른 구체적 처리근거가 있는 경우 등을 제외하고는 법 시행일로부터 2년 이내('16. 8. 6)에 보유하고 있는 주민등록번호를 파기하여야 합니다. 만약 이 기간 내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 「개인정보 보호법」제24조의2제1항을 위반한 것으로 봅니다(「개인정보 보호법」부칙(법률 제11990호) 제2조).

구체적인 조치 사항을 살펴보면, 주민등록번호의 수집 필요성이 없거나 다른 식별 수단으로 대체 가능한 경우에는 대체 조치하고, 기존에 보유하고 있던 주민등록번호는 파기 조치해야 합니다. 예를 들어 성명 및 주민등록번호를 입력하도록 하던 것을 성명 및 생년월일 등으로 대체하여야 합니다.

주민등록번호 등 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 파기해야 하며(「개인정보 보호법」제21조제2항), 보다 구체적인 방법을 살펴보면 전자적 파일 형태의 경우에는 복원이 불가능한 방법으로 영구 삭제, 기록물 · 인쇄물 · 서면 · 그 밖의 기록매체인 경우에는 파쇄 또는 소각하는 방법으로 파기해야 합니다(「개인정보 보호법」시행령 제16조). 한편 주민등록번호가 기재되어 있는 서면의 경우, 해당 서면 자체를 파기해야 하는지 아니면 서면은 보존하되 주민등록번호만 삭제할 것인지 검토 후 조치해야 합니다.

* 전자적으로 기록된 개인정보는 복원기술을 적용할 경우 그 정보가 복구될 가능성도 있으므로, '복원이 불가능한 방법'으로 영구 삭제하라는 의미는 사회 통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 의미함(표준 개인정보 보호지침 제11조제2항)

다만 계약 또는 거래 등과 관련하여 수집한 주민등록번호는 당사자 간 권리 의무 관계에 미치는 영향 및 관련 법령의 정비 추이 등을 충분히 고려하여 신중하게 파기할 것이 요구됩니다.

관련 법령

「개인정보 보호법」부칙

제2조(주민등록번호 처리 제한에 관한 경과조치) ① 이 법 시행 당시 주민등록번호를 처리하고 있는 개인정보처리자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제24조의2제1항 각 호의 개정규정의 어느 하나에 해당하는 경우는 제외한다.

② 제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제24조의2제1항의 개정규정을 위반한 것으로 본다.

「개인정보 보호법」시행령

제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

06 주민등록번호 일부 정보[앞자리 + 뒷자리 첫째숫자] 사용

Q **저희 회사는 고객으로부터 주민등록번호 앞자리와 뒷자리 첫째숫자까지만 수집하여 사용하려고 합니다. 이런 방식은 허용되는지요?**

A 주민등록번호 13자리 체계를 유지하면서 주민등록번호의 일부를 기호로 처리하는 것도 주민등록번호 처리를 허용하는 구체적 법령근거 없으면 금지됩니다.
다만, 주민등록번호 13자리 체계가 아닌 생년월일과 성별을 별도로 수집하는 것은 허용됩니다.

상세 설명

주민등록번호는 생년월일, 성별, 지역 등을 표시할 수 있는 13자리의 숫자로 작성합니다(「주민등록법」시행규칙 제2조). 주민등록번호 13자리 가운데 앞의 여섯 자리는 백년대를 뺀 생년월일로 이루어지며, 뒤의 일곱 자리 숫자는 출생연대와 성별, 최초 주민등록번호 발급지 지역번호, 일련번호와 검증번호로 이루어집니다.

특히 주민등록번호 앞자리의 생년월일 6자리 및 뒤 첫째숫자(출생연대와 성별)는 주민등록번호 고유체계에 따라 생성되는 것이라고도 볼 수 있고, 출생신고 시 국민이 국가에 신고한 날짜를 토대로 정의되는 숫자 열이기도 합니다. 따라서 주민등록번호의 최초 7자리 숫자는 국가에서 확인한 '생년월일 및 성별'을 나타내는 정보로 보아야 할 것이며, 실제의 출생연월일 등과 다를 수도 있습니다.

그러므로 주민등록번호 앞 6자리는 '주민등록상의 생년월일'이라고 칭해야 할 것이며, 주민등록번호 뒤 첫째 자리 숫자는 '주민등록상의 성별'이라고 해야 할 것입니다.

법령상 구체적 근거가 없는 경우에는 주민등록번호의 일부라도 수집하지 않도록 하는 것이 「개인정보 보호법」의 취지이므로, 법정 연령을 확인할 의무가 있는 등 고객으로부터 수집하려는 생년월일 등이 '주민등록상의 생년월일 및 성별'과 반드시 일치되어야만 할 필요가 있는 경우에도 '주민등록번호'의 앞 뒤 일부 숫자를 수집하는 방식 대신, 생년월일(****년 **월 **일) 및 [성별(남성 또는 여성)]을 기재하도록 하는 것이 바람직합니다.

관련 법령

「주민등록법」

제7조(주민등록표 등의 작성) ①~② (생략)

③시장·군수 또는 구청장은 주민에게 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다.

「주민등록법」시행규칙

제2조(주민등록번호의 작성) 「주민등록법」(이하 "법"이라 한다) 제7조제3항에 따른 주민등록번호는 생년월일·성별·지역 등을 표시할 수 있는 13자리의 숫자로 작성한다.

「개인정보 보호법」

제15조(개인정보의 수집 · 이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

07 주민등록번호 일부 정보[뒷자리 전체 또는 일부] 사용

Q **회원 식별 등을 위해서 주민등록번호 뒤 7자리만 수집 · 이용하려 합니다. 주민등록번호 전체를 수집하는 것이 아니므로 괜찮지 않을까요?**

A 주민등록번호 뒷자리만 수집 · 이용하더라도 허용되지 않습니다. 쉽게 확인 가능한 생년월일 정보와 결합하는 경우 주민등록번호를 알 수 있기 때문입니다.

상세 설명

주민등록번호의 뒤 7자리만 수집 · 이용하는 것은 주민등록번호의 부여 체계를 활용하여 주민등록번호의 고유한 특성, 즉 유일성과 식별성을 이용하는 행위이므로, 이는 주민등록번호 전체를 수집 · 이용하는 경우로 볼 수 있습니다.

따라서 법령에서 주민등록번호의 처리를 요구 · 허용하는 구체적 근거가 없는 경우라면 주민등록번호의 뒤 7자리만이라도 수집 · 이용할 수 없다고 보아야 합니다. 나아가 뒤 7자리 중 일부만 처리하는 경우에도 이와 마찬가지입니다.

08 주민등록번호 처리금지 원칙 위반에 따른 벌칙

Q **주민등록번호 처리금지 원칙을 위반한 경우에는 어떠한 제재를 받게 되나요?**

A 주민등록번호 처리금지 원칙을 위반하여 주민등록번호를 처리한 자에게는 3천만원 이하의 과태료가 부과됩니다.

상세 설명

개인정보 보호법에 따른 주민등록번호 처리금지 원칙을 위반하여, 법령의 구체적 요구 · 허용 근거가 없음에도 불구하고 주민등록번호를 처리한 자에게는 3천만원 이하의 과태료가 부과됩니다(「개인정보 보호법」제75조제2항제4의2).

또한 주민등록번호를 포함하여 개인정보를 목적 외로 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서 영리 또는 부정한 목적으로 개인정보를 제공받은 자에게는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과됩니다(「개인정보 보호법」제71조제2호).

한편, 개인정보처리자가 처리하는 주민등록번호가 분실 · 도난 · 유출 · 변조 또는 훼손된 경우에는 5억원 이하의 과징금이 부과될 수 있습니다. 다만 주민등록번호가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 과징금이 부과되지 않습니다(「개인정보 보호법」제34조의2제1항).

관련 법령

「개인정보 보호법」

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

2. 제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

제34조의2(과징금의 부과 등) ① 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

제 2 장

일상생활 사례

제2장 일상생활 사례

09 홈페이지 회원 가입 · 관리를 위한 주민등록번호 수집

Q **홈페이지 회원 가입을 위하여 성명과 주민등록번호 입력을 통한 실명인증 방식을 적용하고 있습니다. 저희가 주민등록번호를 직접 저장하는 것도 아닌데 이러한 경우도 금지가 되나요?**

A 단지 홈페이지 회원가입을 위한 주민등록번호 처리는 법령의 구체적인 근거가 없으므로 금지됩니다.

상세 설명

사업자 또는 공공기관 등이 홈페이지에서 회원 가입과 관리를 위하여 주민등록번호를 처리하는 것은 법령의 구체적인 근거가 없습니다. 따라서 인터넷 홈페이지 회원 가입과 관리를 위하여 주민등록번호를 수집·이용하는 행위는 「개인정보 보호법」에 따른 '주민등록번호 처리금지 원칙'에 위반되므로 금지됩니다.

이와 관련하여, 이른바 '실명인증' 방식으로 불리우는 성명 및 주민등록번호 입력을 통한 본인인증 방식이 논란이 될 수 있습니다. '실명인증' 방식은 홈페이지 회원가입 메뉴의 실명인증란을 통해 주민등록번호가 입력되기는 하지만, 그 주민등록번호가 저장되지 않고 바로 실명인증기관에 전송되어 성명 및 주민등록번호의 진위 · 일치 여부만을 확인한 후 그 결과값을 회신 · 전송하는 방식이 널리 이용되고 있습니다. 따라서 해당 개인정보처리자가 주민등록번호를 직접 수집하거나 저장하는 것은 아니므로 주민등록번호 처리금지 원칙에 위반되는 것이 아니라는 지적도 있을 수 있습니다.

그러나 주민등록번호 처리금지 원칙은 단순히 수집 · 이용, 저장 등을 금지하는 것이 아니라 제반 주민등록번호 처리행위를 모두 금지하고 있습니다. 따라서 개인정보처리자가 주민등록번호를 저장하는 것이 아닌 '실명인증' 방식이라도 주민등록번호 처리금지 원칙에 위반되는 것은 마찬가지입니다. 따라서, 실명인증 방식을 포함하여 홈페이지에서 회원 가입과 관리를 위하여 주민등록번호를 직접 입력하도록 하거나 수집 · 저장하는 제반 행위가 금지된다는 것을 유의하여야 합니다.

홈페이지 회원가입 신청자에 대해 본인이 맞는지 여부의 확인이나 연령을 확인하기 위한 방법으로는 공인인증서, 아이핀(I-PIN), 휴대전화인증 등 다양한 본인확인 방법이 있으므로 이를 활용할 수 있습니다.

10 법령상 주민등록번호 수집근거가 있는 업무처리를 위해 홈페이지 회원 가입 시 주민등록번호 수집

Q **저희 기관은 법령의 구체적인 근거 규정에 따라 주민등록번호를 수집·이용하고 있습니다. 이러한 경우 홈페이지에서 회원가입을 받는 절차에서 주민등록번호를 받아도 되는 것 아닌지요?**

A 법령에 구체적 근거가 있지 않는 한 단순 회원가입 목적으로 주민등록번호를 수집할 수 없습니다. 아이핀, 휴대전화번호 등 다른 수단으로 본인 여부를 확인해야 합니다.

상세 설명

관련 법령에 구체적인 주민등록번호 처리 근거 규정이 존재하는 등 주민등록번호의 처리 근거가 갖춰진 경우에는 인터넷 홈페이지 회원 가입 시에도 실명인증방식과 같이 주민등록번호를 사용하여도 된다고 생각하기 쉽습니다.

그러나 「개인정보 보호법」은 비록 관련 법령에 구체적인 처리 근거 규정이 존재하는 경우에도 정보주체가 인터넷 홈페이지를 통해 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하도록 의무화하고 있습니다(「개인정보 보호법 제24조의2제2항). 따라서 관련 법령에 구체적인 처리 근거 규정이 있더라도 성명 및 주민등록번호를 입력하는 실명인증 방식을 사용하여서는 아니되며, 공인인증서, 휴대전화인증 등의 대체수단을 사용하여야 합니다. 그리고 회원가입 이후의 단계에서 필요하다면 주민등록번호를 수집하는 절차를 갖추어야 합니다.

관련 법령

「개인정보 보호법」

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

② 생략

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

11 멤버십 회원자격 확인, 포인트 관리 등을 위한 주민등록번호 처리

Q **기업에서 고객에게 멤버십 회원 포인트의 부여와 사용, 관리를 위해 고객 주민등록번호를 수집·이용하여도 되는지요?**

A 멤버십 회원 포인트 관리를 위해 주민등록번호를 수집·이용하는 것은 허용되지 않습니다.

상세 설명

예전에는 백화점, 대형마트 등에서 멤버십 회원 포인트(마일리지) 적립을 위해 주민등록번호를 입력하도록 하고 이를 통해 포인트를 부여하거나 사용하던 모습을 쉽게 볼 수 있었습니다. 그러나, 기업 등에서 멤버십 회원의 포인트 관리를 위하여 각 회원의 주민등록번호를 수집하고 이를 기반으로 회원의 구분 · 식별과 포인트 부여, 사용, 관리 등에 이용하는 것은 그 목적의 적합성이나 대체수단 적용가능성 등을 고려해볼 때 개정「개인정보 보호법」에서 규정한 주민등록번호를 수집 · 이용할 수 있는 경우로 보기 어렵습니다.

즉 멤버십 회원의 포인트 관리 등을 위해 회원(정보주체)의 주민등록번호를 수집 · 이용하는 것은 법령에 구체적인 근거가 있는 것도 아니고, 주민등록번호를 처리하지 않고서는 그 멤버십 포인트 관리 업무를 수행하는 것이 근본적으로 불가능한 경우도 아니기 때문입니다(불가피성 불인정).

따라서 이러한 경우에는 기존의 주민등록번호를 생년월일, 별도로 생성 · 부여하는 회원번호, 아이핀 등으로 대체하여 멤버십 회원 포인트 관리를 위해 이용하고, 기존에 수집하여 보관중인 주민등록번호는 개정「개인정보 보호법」시행 후 2년 이내(2016.8.6.까지) 모두 삭제 조치하여야 할 것입니다.

12 콜센터 상담 시 본인확인을 위한 주민등록번호 이용

Q **기업의 콜센터, A/S센터 등에서 고객 본인 확인을 위해 주민등록번호를 사용할 수 있는지요?**

A 콜센터나 A/S센터 등에서 고객 본인 확인을 위해 주민등록번호를 수집 · 이용하는 것은 허용되지 않으며, 생년월일이나 휴대전화번호 등 다른 정보를 이용해야 합니다.

상세 설명

일반적으로 민간기업이나 공공기관의 콜센터 상담 시에는 해당 통화의 상대방이 고객 본인이 맞는지 여부를 확인하기 위해 전화기를 통해 개인정보를 입력하게 하거나 상담원과 문답을 통해 본인 여부를 확인하고 있습니다.

관계 법령에 콜센터 등에서 고객 본인 확인을 위하여 주민등록번호를 처리하도록 하는 구체적 근거 규정이 존재하는 경우도 거의 없습니다. 또한 기업 등의 입장에서는 고객의 성명, 전화번호, 생년월일, 계좌번호, 신용카드번호 등으로 고객 본인 여부를 충분히 확인할 수 있으므로, 반드시 주민등록번호를 요구하거나 수집해야 할 필요성(불가피성)은 인정되지 않습니다.

따라서 콜센터나 A/S 센터 등은 다른 개인정보의 입력이나 조회를 통해 고객 본인 확인을 해야 하고, ARS 시스템을 통해 주민등록번호를 입력하게 하거나 상담원을 통해 주민등록번호를 확인하도록 하는 등의 행위는 「개인정보 보호법」에 따른 주민등록번호 처리금지 원칙에 위반될 수 있으므로 주의해야 합니다.

13 건물 · 시설 출입관리를 위한 주민등록번호 처리

Q **민간 기업이나 공공기관에서 외부 방문자 출입관리와 신원확인, 또는 출입증 발급을 위해서 주민등록번호를 수집 · 이용할 수 있는지요?**

A 민간 기업이나 일반적인 공공기관에서 건물 · 시설의 출입관리를 위한 목적으로 방문자의 주민등록번호를 수집 · 이용하는 것은 허용되지 않습니다.

상세 설명

민간 기업이나 공공기관의 건물 또는 시설에서는 보안 유지와 시설물 안전 등을 위해서 외부 방문자의 성명, 기본적인 연락처, 방문목적 등의 개인정보를 수집 · 이용 및 기록 · 보관할 필요성이 인정될 수 있습니다. 또한 임시 또는 상시 출입증의 발급 · 관리를 위해서도 마찬가지로 방문자의 개인정보를 수집 · 이용할 필요성이 인정될 수 있습니다.

그러나 대부분의 관계 법령에서도 민간 기업의 건물 · 시설의 출입관리 목적이나 출입증 발급 목적으로 주민등록번호의 처리 근거를 두고 있는 경우는 찾기 어렵습니다. 또한 주민등록번호는 일반적인 성명이나 연락처 정보에 비해 그 중요성이 높으며, 따라서 출입 관리를 위한 목적으로 이를 꼭 수집해야 할 불가피성이 인정되기는 어렵습니다. 따라서 이러한 경우에는 해당 시설이나 건물에 출입하는 외부 방문자의 기본적 신원을 파악할 수 있고 필요시 연락을 취할 수 있는 최소한의 개인정보만 수집 · 이용할 수 있고, 주민등록번호는 수집 · 이용할 수 없다고 해야 할 것입니다.

예를 들어 아파트 단지 등과 같이 주차증을 발급하기 위해 해당 건물 · 시설의 거주자 여부를 확인해야 할 필요성도 있을 수 있습니다. 이러한 때에는 주민등록번호 뒷자리가 마스킹(***) 처리된 공부(公簿) 서류를 요청하거나, 주민등록번호 뒷자리까지 표시되어 있는 경우에는 해당 서류를 접수한 이후에 뒷자리를 삭제 처리하거나, 또는 서류를 확인만 하고 돌려주는 방법 등을 이용할 수 있습니다.

한편, 공공기관의 경우에는 보안 필요성에 따라 보호구역에 대한 접근 · 출입 허가 목적으로 주민등록번호를 수집 · 이용할 수 있는 근거가 관련 법령에 마련되어 있으며(「보안업무규정」제46조제1호 참조), 이를 근거로 하여 각 중앙행정기관 등에서는 출입통제대장 등의 서식에 주민등록번호를 기재하도록 하는 경우가 있습니다.

관련 법령

「보안업무규정」

제46조(고유식별정보의 처리) 각급기관의 장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 제32조제3항에 따른 보호구역 접근·출입 허가에 관한 사무
2. 제33조에 따른 신원조사에 관한 사무

14 주민등록번호가 기재된 신분증의 육안 확인

Q **주민등록번호가 기재된 신분증을 단순히 육안으로 확인한 후 돌려주는 행위도 주민등록번호 처리금지 원칙에 위배되는지요?**

A 신분증에 기재된 주민등록번호를 육안으로 확인하는 행위는 '주민등록번호 처리'에 해당하지 아니하여, 이러한 행위는 주민등록번호 처리금지 원칙에 위배되지 않습니다.

상세 설명

건물의 출입통제 확인, 고객의 본인여부 확인 등을 위하여 대상자의 주민등록증, 운전면허증 등 신분증의 제시를 요구하고, 해당 신분증의 사진이나 주민등록번호 등을 육안으로 확인하여 본인 여부를 확인하는 경우가 종종 있습니다. 또한 건물의 출입통제 시에 신분증을 맡기고 출입증을 받아 들어간 다음에, 용무를 마치고 나오면서 출입증을 반납하고 신분증을 되돌려 받는 경우도 있습니다.

이러한 경우 대상자의 주민등록번호를 열람할 수 있기 때문에 '주민등록번호 처리행위'에 해당하고, 따라서 관련 법령에 구체적인 요구 · 허용 근거가 없는 이상 이러한 신분증 육안 확인 행위는 주민등록번호 처리금지 원칙에 위배되는 것이 아니냐는 의견이 있을 수 있습니다.

그러나 단순히 주민등록번호가 기재된 신분증을 육안으로 확인하고 되돌려주는 행위는 '주민등록번호 처리행위'에 해당되지 않는 것으로 해석하고 있습니다. 따라서 신분증을 단순히 육안 확인하거나, 신분증을 단순 보관하였다가 되돌려 주는 행위 등은 주민등록번호 처리금지 원칙에 위배되지 않습니다(행정자치부, 주민등록번호 수집 금지 제도 가이드라인, 2014).

* 다만 건물 출입이나 출입증 발급 등을 목적으로 주민등록번호를 수집·이용하는 경우는 원칙적으로 주민등록번호 처리금지 원칙에 위배될 수 있음

15 위임장에 주민등록번호 기재

Q **중요한 계약을 해야 하는데 상대방 대리인이 생년월일만 기재된 위임장을 제출합니다. 위임장에는 반드시 주민등록번호가 있어야 효력이 있는 것 아닌지요?**

A 위임장은 반드시 주민등록번호가 적혀 있지 않더라도 이름, 생년월일, 주소 등이 적혀 있어 신분증과 대조하여 신분확인을 할 수 있는 경우에도 효력이 인정됩니다. 따라서 법령상 특별한 요구가 없는 경우에는 위임장에 주민등록번호를 기재하지 않습니다.

상세 설명

본인이 직접 거래를 하지 않고 대리인을 통하여 거래하는 경우 위임장을 통해 상대방에게 대리행위임을 알리는 것이 일반적입니다. 그런데 우리나라에서는 오랜 기간 중요한 거래나 법률행위를 위임하는 경우 위임장에 본인과 대리인의 인적사항을 기재하면서, 주민등록번호를 반드시 써야 하는 것으로 오인해 왔습니다.

그러나 매우 특수한 사유로 본인 또는 대리인의 주민등록번호를 반드시 수집하여야 하는 경우에는 관련 법령상 근거가 마련되어 있으며, 그 밖에 대부분의 대리행위에는 위임장에 본인 또는 대리인의 주민등록번호를 기재할 법령상 근거도 없고 그러한 불가피성도 없습니다.

예를 들어 개인정보의 열람요구나 정정·삭제 요구와 같은 중요한 행위를 대리할 때에도 「개인정보 보호법」 시행규칙에 따라 정보주체와 대리인의 [성명, 전화번호, 생년월일, 주소]만 기재하도록 하고 있습니다(별지 제8호서식).

따라서 위임장에 주민등록번호가 기재되지 않았다고 하여 법적인 효력이 없는 것은 아니며, 오히려 주민등록번호가 아닌 생년월일의 기재가 바람직한 것입니다.

한편 다음과 같은 특수한 업무의 위임에는 관련 법령의 종합적 검토를 통하여 위임인 또는 수임인의 주민등록번호 처리의 적법성 여부를 판단하게 됩니다.

예를 들어, 개인회생, 파산 및 면책신청을 전문으로 하는 업무를 수임한 자는 의뢰인인 채무자를 대신하여 해당 채무자의 부채증명 발급을 금융기관에 요구하게 되는데, 이때 채무자의 주민등록번호는 「금융실명거래 및 비밀보장에 관한 법률」 등 금융관계

법령에서 정하는 바에 따라 이미 금융기관이 적법하게 수집 · 관리하고 있는 정보라는 점, 「개인정보보호법」 제4조 제3호에 따라 정보주체는 자신의 개인정보에 대한 처리 여부를 확인하고 그 개인정보에 대한 열람 또는 사본의 발급을 요구할 권리를 가지고 있는 점 등을 고려할 때, 수임인이 채무자의 명시적 요청에 따라 부채증명을 발급받기 위한 경우라면 해당 채무자의 주민등록번호가 포함된 자료를 금융회사에 제출하는 것은 「개인정보 보호법」에 저촉되지 아니할 것이지만, 채무자의 의뢰를 받은 수임인의 주민등록번호는 금융관계 법령에서 정하는 바에 따라 금융기관이 구체적으로 요구하거나 제출받을 수 있는 정보로 보기 어려운 바, 원칙적으로 금융기관이 법령상 근거 없이 수임인의 주민등록번호가 기재된 위임장 등의 서류를 요구하거나 제출받는 행위는 「개인정보 보호법」에 저촉될 수 있습니다.

관련 법령

「개인정보 보호법」시행규칙 별지 제8호 서식 (개인정보(열람, 정정·삭제, 처리정지) 요구서)

개인정보([ ]열람 [ ]정정 · 삭제 [ ]처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호		접수일	처리기간 10일 이내
정보주체	성 명		전 화 번 호
	생년월일		
	주 소		
대리인	성 명		전 화 번 호
	생년월일		정보주체와의 관계
	주 소		

16 법무·노무사건 위임 시 주민등록번호 처리

Q **법무사나 노무사에게 사건을 위임할 때 주민등록번호를 알려주는 게 적법한 것인지요?**

A 법무사건이나 노무사건과 같이 관련 법령상 위임인의 주민등록번호를 처리해야 업무가 가능한 경우, 수임인이 위임인의 주민등록번호를 수집할 수 있습니다.

상세 설명

다음과 같은 특수한 업무의 위임에는 각각 관련 법령의 종합적 검토를 통하여 위임인 또는 수임인의 주민등록번호 처리의 적법성 여부를 판단하게 됩니다.

예를 들어, 법무사가 정보주체(위임인)의 명시적 위임을 받아 당해 정보주체를 대신하여 작성하는 각종 신청서 등에 해당 정보주체의 주민등록번호를 기재하거나, 당해 정보주체를 대신하여 해당 정보주체의 주민등록번호가 기재된 신청서를 법원 등 관계 법령상 주민등록번호 수집이 허용된 기관에 제출하는 경우, 「법원재판사무 처리규칙」 제5조의2, 「법원 개인정보 보호에 관한 규칙」 제5조, 「민사소송규칙」 제76조의2, 「형사소송규칙」 제132조의5 등에 따라 법원 또는 법원행정처는 민 · 형사 소송이나 재판, 등기 관련 사무 등을 처리하기 위하여 필요한 범위 내에서 주민등록번호를 처리(수집 · 이용 등)할 수 있다고 규정하고 있는 점, 「법무사법」 제2조에 따라 법무사는 다른 사람이 위임한 사무를 수행하는 것을 업무로 하는 자에 해당한다는 점을 종합적으로 고려할 때 「개인정보 보호법」에 합치된다고 해석됩니다.

또한 공인노무사가 사업주 또는 근로자로부터 명시적 위임 또는 위탁을 받아 당해 사업주 또는 근로자를 대신하여 각종 신청 · 신고 등의 사무를 처리하는 과정에서 노동관계 법령에서 정하는 바에 따라 신청 · 신고 대상자의 주민등록번호를 고용노동부, 근로복지공단, 국민건강보험공단, 노동위원회 등 주민등록번호 수집이 허용된 기관에 제출하는 경우도 「고용보험 및 산업재해보상보험의 보험료 징수에 관한 법률 시행령」 제19조의5, 「산업재해보상보험법 시행령」 제127조의2, 「근로기준법 시행령」 제59조의2, 「국민건강보험법 시행령」 제81조에 따라 고용노동부, 근로복지공단, 국민건강보험공단, 노동위원회 등은 보수총액 신고, 보험급여 지급 신청, 법 위반 사실 통보, 자격 취득 및 변경 신고 등의 사무를 수행하기 위하여 주민등록번호를 처리(수집 · 이용 등)할 수 있다고 규정하고 있는 점, 「공인노무사법」 제2조제1호에 따라 공인노무사는 노동 관계 법령에 따라 관계 기관에 대하여 행하는 각종 신청 등의 대행 또는 대리 등의 직무를 수행하는 자에 해당한다는 점을 종합적으로 고려할 때, 「개인정보 보호법」에 합치된다고 해석됩니다.

다만 관련 법령상 위임인의 주민등록번호를 기재 등 처리하지 않고도 업무가 가능한 경우에는, 수임인이 위임인의 주민등록번호를 수집하지 않도록 하여야 할 것입니다.

17 현금영수증 처리를 위하여 주민등록번호 처리

Q 현금영수증 처리를 주민등록번호로 하는 것도 적법한 것인지요?

A 조세특례제한법에 따른 현금영수증 사업자의 경우에만 현금영수증 발행을 위하여 정보주체의 주민등록번호를 수집할 수 있습니다.

상세 설명

고객이 현금결제 후 현금영수증 발행을 요청할 때, 휴대폰번호를 이용하는 것이 일반적이나, 간혹 주민등록번호를 이용하여 현금영수증 발행을 요청할 때도 있습니다.

우선, 2014.8.7.부터 시행된 현행 「개인정보 보호법」 제24조의2에 따라 고유식별정보 중 주민등록번호의 경우에는 아무리 정보주체의 동의가 있는 경우라 하더라도 법령상 근거 없이 주민등록번호를 수집·이용 할 수 없으며, 법령(법률, 시행령, 시행규칙)에서 구체적으로 주민번호 처리를 요구·허용하는 경우 등에 한하여 엄격히 그 처리가 제한됩니다.

다만, 「조세특례제한법」에 따른 현금영수증 사업자(현금영수증 결제를 승인하고 전송할 수 있는 시스템을 갖춘 사업자로서, 대통령령으로 정하는 바에 따라 국세청장으로부터 현금영수증사업의 승인을 받은 자)는 「조세특례제한법」에 따라서 주민등록번호 수집 · 이용이 가능합니다.

그러나 현금영수증 사업자가 아닌 일반 사업자의 경우에는 고객의 요청이 있다 하더라도 현금영수증 발행을 위해 주민번호를 수집·이용 할 수 있는 법령상 구체적인 근거가 있다고 할 수 없는 바, 이 경우에는 주민번호 처리가 금지되며 현금영수증 발행업체에서 직접 제공하는 입력창을 통해서만 이용자의 정보를 제공 받을 수 있습니다.

관련 법령

「조세특례제한법」

제126조의3(현금영수증사업자 및 현금영수증가맹점에 대한 과세특례) ① 현금영수증 결제를 승인하고 전송할 수 있는 시스템을 갖춘 사업자로서 대통령령으로 정하는 바에 따라 국세청장으로부터 현금영수증사업의 승인을 받은 현금영수증사업자(이하 이 조에서 "현금영수증사업자"라 한다)는 대통령령으로 정하는 현금영수증발급장치 설치 건수, 신용카드단말기 등에 현금영수증발급장치를 설치한 사업자(이하 이 조에서 "현금영수증가맹점"이라 한다)의 현금영수증 결제 건수 및 「소득세법」 제164조제3항 후단에 따른 방법으로 제출하는 지급명세서의 건수에 따라 대통령령으로 정하는 금액을 해당 과세기간의 부가가치세 납부세액에서 공제받거나 환급세액에 가산하여 받을 수 있다.

② 제1항에 따른 현금영수증가맹점이 제4항에 따른 현금영수증(거래건별 5천원 미만의 거래만 해당하며, 발급승인 시 전화망을 사용한 것을 말한다)을 발급하는 경우 해당 과세기간별 현금영수증 발급건수에 대통령령으로 정하는 금액을 곱한 금액(이하 이 조에서 "공제세액"이라 한다)을 해당 과세기간의 소득세 산출세액에서 공제받을 수 있다. 이 경우 공제세액은 산출세액을 한도로 한다.

③ 현금영수증사업자는 거래일시, 금액, 거래자의 인적사항 및 현금영수증가맹점의 인적사항 등 현금결제와 관련한 세부 내용을 대통령령으로 정하는 바에 따라 국세청장에게 전송하여야 한다.

④ 제1항에 따른 "현금영수증"이란 현금영수증가맹점이 재화 또는 용역을 공급하고 그 대금을 현금으로 받는 경우 해당 재화 또는 용역을 공급받는 자에게 현금영수증 발급장치에 의해 발급하는 것으로서 거래일시·금액 등 결제내용이 기재된 영수증을 말한다.

⑤ 국세청장은 현금영수증을 발급받은 자의 소득공제 등 현금영수증제도 운영을 위하여 필요한 경우에는 「신용정보의 이용 및 보호에 관한 법률」 제14조에 따라 성명·주민등록번호 등 대통령령으로 정하는 정보의 제공을 같은 법 제2조에 따른 신용정보제공·이용자에게 요청할 수 있다.

⑥ 그 밖에 현금영수증 발급방법 및 그 양식, 제2항에 따른 세액공제의 방법과 절차 등 현금영수증제도 운영에 필요한 사항은 대통령령으로 정한다.

제 3 장

공공 행정 사례

제3장 공공 행정 사례

18 특허출원 청구 시 주민등록번호 기재

Q 특허청에 특허출원 청구를 하는 경우에 주민등록번호를 꼭 기재해야 하는지요?

A 특허출원을 청구하려는 자는 특허법 시행령에 따라 우선 성명, 주민등록번호, 주소 등을 기재하여 고유번호를 부여받은 후, 그 고유번호를 기재한 출원서를 제출하여야 합니다.

상세 설명

특허출원을 청구하는 자는 특허청장 또는 특허심판원장에게 「특허법 시행규칙」에 따른 '특허출원서'를 제출하여야 하는데, 이 출원서에는 반드시 [출원인코드]를 기재하도록 하고 있습니다(별지 제14호서식).

따라서 「특허법」제28조의2는 특허에 관한 절차를 밟는 자 중 일정한 자는 특허청장 또는 특허심판원장에게 자신의 고유번호 부여를 신청하도록 하고 있는데, 이 고유번호는 「특허법 시행규칙」제9조에 따라 '출원인코드부여신청서' 제출하여 부여받게 됩니다.

그런데 '출원인코드부여신청서'에는 제출인의 [성명, 주민등록번호, 전화번호, 주소] 등을 기재도록 하고 있습니다(「특허법 시행규칙」 별지 제4호서식).

또한 특허청장 등은 특허출원에 관한 사무 등 「특허법 시행령」 제19조의2에 각호 소정의 사무를 수행하기 위하여 불가피한 경우 주민등록번호를 처리할 수 있도록 규정되어 있습니다.

그러므로 특허출원을 청구하기 위하여 직접 특허출원서에 주민등록번호를 기재해야 하는 것은 아니지만, 특허출원서를 제출하기에 앞서 출원인코드부여를 받기 위해서는 해당 신청서에 주민등록번호를 기재하도록 하고 있고, 이는 법령에 명확한 근거가 있는 것이므로, 구체적 근거법령을 토대로 주민등록번호를 처리하는 경우에 해당됩니다.

관련 법령

「특허법 시행령」

제19조의2(고유식별정보의 처리) 특허청장 또는 특허심판원장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우「개인정보 보호법 시행령」제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제28조의2에 따른 고유번호의 부여에 관한 사무
2. 법 제42조에 따른 특허출원에 관한 사무
3. 법 제157조에 따른 증거조사 및 증거보전에 관한 사무
4. 법 제222조에 따른 서류의 제출 등에 관한 사무
5. 그 밖에 법 및 이 영에 따른 출원, 심사, 심판, 등록에 관한 신청·신고 또는 제출에 관한 사무

「특허법」

제28조의2(고유번호의 기재) ① 특허에 관한 절차를 밟는 자 중 산업통상자원부령으로 정하는 자는 특허청장 또는 특허심판원장에게 자신의 고유번호의 부여를 신청하여야 한다.

「특허법 시행규칙」

제9조(출원인코드의 부여등) ① 법 제28조의2제1항에서 "산업통상자원부령이 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 출원인
2. 특허를 받을 수 있는 권리의 승계인
3. 심사청구인(이하 생략)

「특허법」시행규칙 별지 제4호 서식 (출원인코드부여신청서)

■ 특허법 시행규칙 [별지 제4호서식] <개정 2014.6.27>

특허로(www.patent.go.kr)에서 온라인으로 제출 가능합니다.

출원인코드부여신청서

(앞쪽)

【제출인】
【성명(명칭)의 국문표기】
【성명(명칭)의 영문표기】
【제출인 구분】
(【주민등록번호】)
【전화번호】
【우편번호】
【주소】
(【전자우편주소】)
(【휴대전화번호】)
【제출인 인감(서명)】

19 공공기관에 '다수인 관련 민원' 제기 시, 주민등록번호 기재

Q **공공기관에 다수인이 민원을 제기하는 경우에는 연명부(連名簿)를 제출해야 하는데, 이때 연명부에 주민등록번호를 꼭 기재해야 하는지요?**

A '다수인 관련 민원'을 제기하기 위해 연명부를 작성 · 제출하는 경우에는 주민등록번호를 기재할 필요가 없습니다.

상세 설명

5세대 이상의 공동 이해와 관련되어 5인 이상이 연명으로 제출하는 민원을 '다수인 관련 민원'이라고 부릅니다. 다수인 관련 민원은 이해관계가 첨예하게 대립하거나 공익 또는 국가정책과 밀접하게 관련된 민원이 많고, 특히 대규모 개발사업이나 비선호 시설 등과 관련하여 빈번히 발생하고 있습니다.

행정기관의 장은 다수인 관련 민원이 발생하지 않도록 사전예방대책을 마련하고, 다수인 관련 민원이 발생한 경우에는 신속 · 공정하게 해결될 수 있도록 조치하여야 할 의무가 있습니다(「민원사무 처리에 관한 법률」시행령 제22조제1항). 그리고, 다수인 관련 민원을 신청하는 민원인은 연명부를 원본으로 제출하여야 합니다(「민원사무 처리에 관한 법률」시행령 제22조제2항).

과거에는 다수인 민원 신청을 주도하는 주민 대표 등이 연명부 서식에 주민등록번호 기재를 요구하는 경우가 종종 있어 왔습니다. 그러나 「민원사무 처리에 관한 법률」시행령은 '행정기관에 특정한 행위를 요구하는 자로서 성명 · 주소 등이 분명하지 아니한 자'를 민원인으로 보지 않는 규정을 두고 있을 뿐이므로(「민원사무 처리에 관한 법률」시행령 제2조제1항제3호), 다수인 관련 민원이라 하더라도 연명부에 성명과 주소 등만 기재하면 되고 주민등록번호를 기재할 법적 근거는 없습니다. 따라서 다수인 관련 민원을 제기하는 경우에는 연명부에 주민등록번호를 기재할 필요가 없습니다.

* 다수인 관련 민원은 반드시 연명부를 원본으로 제출해야 하며, 별도의 서명 없이 자필로 성명을 기록한 경우에는 이를 서명으로 볼 수 있음 (국민신문고 홈페이지 www.epeople.go.kr → 민원 · 정책 Q&A 참조)

관련 법령

「민원사무 처리에 관한 법률」시행령

제2조(정의) ① 다음 각 호의 어느 하나에 해당하는 자는 「민원사무 처리에 관한 법률」(이하 "법"이라 한다) 제2조제1호에 따른 "민원인"으로 보지 아니한다.

1. ~ 2. (생략)

3. 행정기관에 특정한 행위를 요구하는 자로서 성명·주소 등이 분명하지 아니한 자

제22조(다수인 관련 민원의 관리) ① 행정기관의 장은 5세대 이상의 공동이해와 관련되어 5인 이상이 연명으로 제출하는 민원(이하 "다수인관련민원"이라 한다)이 발생하지 않도록 사전예방대책을 마련하여야 하며, 다수인관련민원이 발생한 경우에는 신속·공정하게 해결될 수 있도록 조치하여야 한다.

② 제1항에 따라 다수인관련민원을 신청하는 민원인은 연명부(　)를 원본으로 제출하여야 한다.

(이하 생략)

20 훈장 · 포장, 정부 표창의 공적심사를 위한 주민등록번호 처리

Q **훈장 · 포장이나 정부 표창을 수여하는 경우에는 표창 대상자의 공적을 심사하는 절차가 있는데, 이를 위하여 대상자의 주민등록번호를 수집 · 이용할 수 있는지요?**

A 대한민국 훈장 · 포장 및 정부 표창 수여를 위한 공적심사 목적으로 수상 대상자의 주민등록번호를 수집 · 이용하는 것은 상훈법 시행령에 따라 허용됩니다.

상세 설명

대한민국 국민이나 우방국 국민으로서 대한민국에 뚜렷한 공적을 세운 사람에게 훈장 및 포장을 수여할 수 있으며(「상훈법」제2조 참조), 정부는 국가 또는 사회에 공헌한 행적이 뚜렷한 내외국인이나 교육 · 경기 및 작품 등에서 우수한 성적을 발휘한 자에게 표창을 수여할 수 있습니다(「정부 표창 규정」제2조 참조).

훈장 및 포장의 경우 중앙행정기관의 장, 국회사무총장, 법원행정처장, 헌법재판소사무처장 및 중앙선거관리위원회사무총장이 서훈을 추천하며, 이 외의 서훈의 추천은 행정자치부장관이 합니다. 서훈의 추천은 공적심사위원회의 공적심사를 거쳐 공적조서가 제출되어야 하며, 필요한 경우에는 서훈 대상자의 동의를 받아 관계 법령에서 정하는 바에 따라 서훈 대상자의 범죄경력과 그 밖의 필요한 정보를 해당 정보보유기관의 장에게 요청할 수 있습니다(「상훈법」제5조, 동법 시행령 제2조). 정부 표창의 경우 표창권자는 대통령, 국무총리와 각 중앙행정기관의 장 및 각급 기관의 장이 되며, 역시 공적심사위원회를 통하여 표창 대상자의 공적조서에 의한 공적을 심사하여야 합니다(「정부 표창 규정」제13조).

한편 「상훈법」 및 동법 시행령, 「정부 표창 규정」은 훈장 · 포장 및 정부 표창의 수여와 공적심사와 관련하여 주민등록번호의 수집 · 이용 등에 대한 직접적인 규정을 두고 있지는 않으나, 동 법령들에서 정하는 '공적조서'(별지서식)은 훈장 · 포장 서훈 대상자 및 정부 표창 수여 대상자의 공적심사를 위하여 주민등록번호를 기재하도록 하고 있습니다. 따라서 훈장 · 포장 서훈 및 정부 표창의 공적심사 등을 위하여서는 주민등록번호를 수집 · 이용할 수 있습니다.

관련 법령

「상훈법」시행령 별지 제1호 서식 (공적조서)

■ 상훈법 시행령 [별지 제 1호서식] <개정 2013.1.16>

공적조서

(앞 쪽)

성 명	(한자)		
주 민 등 록 번 호		군번(군인인경우)	
		국적(외국인인 경우)	

「정부 표창 규정」별지 제4호 서식 (공적조서)

■ 정부 표창 규정[별지 제4호서식] <개정 2013.1.16>

공적조서 [ ] 공적상 [ ] 참안상 [ ] 협조상

(앞 쪽)

성 명	(한자)		
주 민 등 록 번 호		군번(군인인경우)	
		국적(외국인인 경우)	

21 기초생활수급자, 장애인 등 사회적 배려대상자에 대한 공공요금 경감을 위한 주민등록번호 처리

Q **사회적 배려 대상자에 대해 전기, 가스, 수도 등 공공요금의 감면 혜택을 제공하기 위해 주민등록번호를 수집 · 이용할 수 있는지요?**

A 사회적 배려대상자에 대한 공공요금 경감은 각 중앙행정기관 · 지방자치단체 및 해당 역무를 제공하는 공기업 별로 이루어지고 있으며, 대체로 업무를 위한 주민등록번호 처리근거가 관련 법령에 마련되어 있으므로 허용되는 경우가 많습니다. 구체적 법령근거를 확인하려면 해당기관의 개인정보보호 책임자에게 문의하시면 됩니다.

상세 설명

일정한 자격을 갖춘 사회적 배려대상자에 대해서는 복지정책 차원에서 전기, 가스, 수도 등 공공요금에 대한 경감 · 할인 혜택이 제공되고 있습니다. 공공요금 경감 혜택을 받는 대상자는 「장애인복지법」에 따른 장애인, 「국민기초생활 보장법」에 따른 국민기초생활보장수급자 및 차상위계층, 「국가유공자 등 예우 및 지원에 관한 법률」에 따른 국가유공자 등이 있습니다.

* 국민기초생활보장수급자 및 장애인 등에 대한 공공요금 감면 상세 내역은 보건복지부(www.mw.go.kr) 홈페이지 → 정책 → '복지' 또는 '장애인' 메뉴 → '각종감면제도안내'를 참조

* 국가유공자 등에 대한 공공요금 감면 상세 내역은 국가보훈처(www.mpva.go.kr) 홈페이지 → '보훈지원' 메뉴를 참조

각각의 근거 법률은 해당 지원 대상자에 대해 경제적 부담의 경감을 위한 지원과 정책 강구 의무를 기본적으로 규정하고 있습니다. 예를 들어 「장애인복지법」은 국가, 지방자치단체, 공공기관, 지방공사 또는 지방공단으로 하여금 장애인 및 장애인을 부양하는 자의 경제적 부담을 줄이고 장애인 자립을 촉진하기 위해 세제상의 조치, 공공시설 이용료 감면, 그 밖에 필요한 정책을 강구하도록 의무를 부과하고 있습니다(「장애인복지법」제30조).

이러한 원칙에 따라서, 각 중앙행정기관 및 지방자치단체 등에서는 각종 경감혜택을 시행하고 있습니다. 예를 들어 산업통상자원부는 '사회적 배려대상자에 대한 도시가스요금 경감지침'을 통하여 1~3급 장애인, 1~3급 상이자, 독립유공자 또는 수급자, 기초생활수급자, 차상위계층 중 일정 요건을 충족하는 자, 다자녀가구 등에 대해 도시가스요금을 경감하도록 하고, 경감을 희망하는 자는 자신이 사회적 배려대상자임을 입증할 수 있는 증빙서류와 함께 신청서를 제출하도록 규정하고 있습니다.

2014.8.7. 이전에는 이러한 공공요금 경감을 위한 주민등록번호 처리의 구체적 허용근거가 관계 법령이 아닌 각 부처의 지침이나 고시 또는 각 지차체의 조례 등에 산재하였으나, 해당

업무에 주민등록번호 처리의 불가피성이 인정되어 관련 법령의 정비가 진행되었습니다.

따라서 이제는 사회적 배려대상자, 저소득층 또는 장애인에 대한 각종 공공요금 경감을 위해 대상자의 주민등록번호를 처리할 수 있다는 명시적 근거 규정이 존재하는 경우가 대부분입니다.

다만 근거 법령이 존재하지 않는 한 아무리 복지서비스 제공을 위한 경우라 하더라도 주민등록번호를 수집 · 이용할 수 없다고 해야 할 것이며, 이러한 경우에는 복지 수혜자격자임을 입증할 수 있는 각종 서류(주민등록등본, 장애인증명서, 기초생활수급자증명서 등)를 첨부 · 접수한 경우에도 주민등록번호 뒷자리가 마스킹 처리된 서류를 요구하거나 또는 뒷자리를 삭제 조치하여 접수 · 보관할 필요가 있습니다.

관련 법령

「장애인복지법」

제30조(경제적 부담의 경감) ① 국가와 지방자치단체, 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관, 「지방공기업법」에 따른 지방공사 또는 지방공단은 장애인과 장애인을 부양하는 자의 경제적 부담을 줄이고 장애인의 자립을 촉진하기 위하여 세제상의 조치, 공공시설 이용료 감면, 그 밖에 필요한 정책을 강구하여야 한다.

②국가와 지방자치단체, 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관, 「지방공기업법」에 따른 지방공사 또는 지방공단이 운영하는 운송사업자는 장애인과 장애인을 부양하는 자의 경제적 부담을 줄이고 장애인의 자립을 돕기 위하여 장애인과 장애인을 보호하기 위하여 동행하는 자의 운임 등을 감면하는 정책을 강구하여야 한다.

「전기통신사업법」시행령

제65조의2(고유식별정보의 처리) ② 기간통신역무를 제공하는 전기통신사업자 또는 한국정보통신진흥협회는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. 〈신설 2014.8.6., 2015.4.14.〉

1. 법 제4조 및 이 영 제2조제2항제3호에 따른 요금감면 서비스 제공에 관한 사무
2. 법 제29조에 따른 요금의 감면에 관한 사무
3. 법 제50조제1항제5호에 따른 금지행위 중 이용자의 가입의사를 확인하지 아니하고 이용계약을 체결하는 행위 및 이용약관(요금 반환에 관한 내용만 해당한다)과 다른 전기통신서비스를 제공하는 행위를 예방하기 위한 사무

22 지자체 일자리사업 참여자의 주민등록번호 처리

Q **취업취약계층 우선 선발을 위해 일자리사업 참여자의 주민등록번호를 이용하는 재산조회가 허용되는 것인지요?**

A 고용정책기본법 등에 근거하여 해당 신청자의 주민등록번호를 이용하여 재산조회를 실시하는 것은 허용됩니다.

상세 설명

고용정책기본법 제6조에 따라 지방자치단체 국고보조사업으로 추진되는 지역공동체일자리사업에서는 일정 생활수준 이하의 신청자를 선발하기 위해 참여자의 재산조회가 필요하게 됩니다.

이 사업은 고용정책기본법을 관할하는 고용노동부가 총괄하고 있으며 지자체가 고용노동부와 업무위탁(또는 협약)을 체결한 후 신청자 재산조회를 하게 되는데, 이 때 고용노동부의 “일모아시스템”에 주민등록번호를 이용하게 됩니다.

고용정책기본법 시행령 제43조의2에 따라 고용노동부장관은 “재정지원일자리사업”을 통합 관리하는 정보전산망 운영에 관한 사무 등을 수행하기 위하여 불가피한 경우 주민등록번호 등을 처리할 수 있다고 규정하고 있는 점, 지방자치단체가 국고보조사업으로 수행하는 지역공동체일자리사업은 고용노동부가 고용정책기본법 제13조의2에 따라 수행하는 ‘재정지원일자리사업’에 포함된다는 점, 고용노동부가 발간한 ‘2014년도 재정지원일자리사업 중앙부처-자치단체 합동지침’에서는 취업취약계층을 우선 선발토록 하면서“일모아시스템”에 신청자 성명, 주민등록번호 등을 입력하여 참여자 선발을 관리하도록 정하고 있는 점 등을 종합적으로 고려할 때, 지자체가 개인정보보호법 제26조에 따른 업무위탁 절차를 준수하여 고용노동부의 업무를 수탁받아 수행하는 경우라면 그 수탁업무의 범위 내에서 신청자 본인의 명시적 동의하에 해당 신청자의 주민등록번호를 고용노동부의 “일모아시스템”에 입력하여 재산조회를 실시하는 것은 개인정보보호법에 저촉되지 아니할 것으로 판단됩니다.

23 희귀난치성질환자 의료비지원사업 참여자의 주민등록번호 처리

Q **희귀난치성질환자 의료비지원사업 대상자의 자격확인과 의료비 지원을 위하여 신청자의 주민등록번호를 수집할 수 있는 것인지요?**

A 희귀난치성 질환자 등을 대상으로 하는 사회복지서비스 신청 및 조사, 서비스 제공 실시 등의 사무를 수행하기 위하여 불가피한 경우에는 희귀난치성질환 의료비지원 신청자의 주민등록번호를 처리할 수 있습니다.

상세 설명

질병관리본부는 희귀난치성질환자와 그 가계의 경제적 파탄을 방지하고자 '희귀난치성 의료비지원사업'을 수행하고 있으며, 동 사업 대상자(건강보험가입자 중 저소득층 해당)의 자격 확인과 의료비 지원을 위하여 본인 동의를 받아 주민등록번호를 수집 · 활용하고 있습니다.

이 사업은 「사회복지사업법」 제33조의3 제1항은 시장 · 군수 · 구청장이 같은 법 제33조의2에 따른 사회복지서비스 제공 신청을 받으면 복지담당공무원에게 같은 법 제2조제1호에 따른 사회복지사업 중 보건복지부령으로 정하는 수혜이력에 관한 사항을 조사하게 하도록 규정하고 있는 점, 같은 법 시행규칙 제19조의3 제2항은 위 수혜이력 조사에 있어 희귀난치성 질환을 가진 사람에 대한 지원 이력 등을 포함하고 있는 점, 보건복지부가 발행한 '2014년도 희귀난치성질환자 의료비지원사업 지침' 별지 제5호 서식은 희귀난치성질환 의료비지원 신청자의 개인정보를 「사회복지사업법」 제33조의3에 따른 복지대상자 선정 등을 위한 목적으로 활용함을 밝히고 있는 점 등을 종합적으로 고려할 때, 「사회복지사업법」 제2조 제6호에 따른 사회복지서비스의 범위에 포함될 수 있습니다

따라서, 보건복지부 장관 또는 지방자치단체의 장(해당 업무가 소속기관 또는 산하기관에 위임 · 위탁된 경우에는 수임 · 수탁받은 기관을 포함)이 희귀난치성 질환자 등을 대상으로 하는 사회복지서비스 신청 및 조사, 서비스 제공 실시 등의 사무를 수행하기 위하여 불가피한 경우에는 「사회복지사업법 시행령」 제25조의2제2항에 따라 주민등록번호를 처리(수집 · 이용 · 제공 등)할 수 있으며, 이러한 경우는 「개인정보보호법」 제24조의2에 저촉되지 아니할 것으로 판단됩니다.

24 보육교사 교육 및 자격증 발급을 위한 주민등록번호 처리

Q **보육교사 양성교육을 하고 있는 기관입니다. 현재 보육교사 자격증 발급과 관리 업무를 위해 주민등록번호를 수집하고 있는데 문제가 없는지요?**

A 영유아 보육교사의 자격증 신청과 관리를 위해서는 영유아보호법 등에 근거가 있으므로 주민등록번호의 수집 · 이용이 허용됩니다.

상세 설명

어린이집의 원장 및 보육교사는 일정 자격을 가진 자로서 보건복지부장관이 검정 · 수여하는 자격증을 받은 자이어야 합니다. 특히 보육교사의 경우에는 1) 「고등교육법」 제2조에 따른 학교에서 보건복지부령으로 정하는 보육 관련 교과목과 학점을 이수하고 전문학사학위 이상을 취득한 사람, 2) 법령에 따라 「고등교육법」 제2조에 따른 학교를 졸업한 사람과 같은 수준 이상의 학력이 있다고 인정된 사람으로서 보건복지부령으로 정하는 보육 관련 교과목과 학점을 이수하고 전문학사학위 이상을 취득한 사람, 3) 고등학교 또는 이와 같은 수준 이상의 학교를 졸업한 자로서 시·도지사가 지정한 교육훈련시설에서 소정의 교육과정을 이수한 사람 중 어느 하나에 해당하고 보건복지부장관이 검정 · 수여하는 자격증을 받아야 합니다(「영유아보육법」제21조). 보육교사자격 취득을 위한 '교육훈련시설'은 시 · 도지사가 지방보육정책위원회의 심의를 거쳐 지정합니다(「영유아보육법」시행규칙 제13조). 보건복지부장관은 어린이집 원장 또는 보육교사의 자격을 검정하고 자격증을 교부합니다(「영유아보육법」제22조).

이와 관련하여 「영유아보육법」시행령은 보건복지부장관 또는 지방자치단체의 장, 그리고 이들로부터 권한을 위임 · 위탁받은 자로 하여금 '어린이집의 원장 또는 보육교사의 자격검정 및 자격증 교부에 관한 사무' 등을 위하여 불가피한 경우에는 주민등록번호 등을 처리할 수 있도록 명시적인 규정을 두고 있습니다(「영유아보육법」시행령 제26조의3). 또한 동법 시행규칙은 어린이집 원장 또는 보육교사의 자격증 발급 · 재발급 신청서, 자격증 서식 등에 주민등록번호를 기재하도록 하고 있습니다.

따라서 보육교사 교육훈련시설 등에서 보육교사자격 취득, 신청, 관리 등을 위하여 대상자의 주민등록번호를 수집 · 이용하는 것은 '법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'에 해당하므로, 이 때에는 보육교사 교육대상자 등의 주민등록번호를 수집 · 이용할 수 있습니다.

관련 법령

「영유아보육법」

제21조(어린이집의 원장 또는 보육교사의 자격) ① 어린이집의 원장은 대통령령으로 정하는 자격을 가진 자로서 보건복지부장관이 검정·수여하는 자격증을 받은 자이어야 한다.

② 보육교사는 다음 각 호의 어느 하나에 해당하는 자로서 보건복지부장관이 검정·수여하는 자격증을 받은 자이어야 한다.

1. 「고등교육법」 제2조에 따른 학교에서 보건복지부령으로 정하는 보육 관련 교과목과 학점을 이수하고 전문학사학위 이상을 취득한 사람

1의2. 법령에 따라 「고등교육법」 제2조에 따른 학교를 졸업한 사람과 같은 수준 이상의 학력이 있다고 인정된 사람으로서 보건복지부령으로 정하는 보육 관련 교과목과 학점을 이수하고 전문학사학위 이상을 취득한 사람

2. 고등학교 또는 이와 같은 수준 이상의 학교를 졸업한 자로서 시·도지사가 지정한 교육훈련시설에서 소정의 교육과정을 이수한 사람

「영유아보육법」시행령

제26조의3(민감정보 및 고유식별정보의 처리) ① 보건복지부장관(제26조 및 제26조의2에 따라 보건복지부장관의 권한을 위임·위탁받은 자를 포함한다) 또는 지방자치단체의 장(해당 권한이 위임·위탁된 경우에는 그 권한을 위임·위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

5. 법 제19조에 따른 보육교직원의 임면 및 경력 등의 관리에 관한 사무

6. 법 제21조 및 제22조에 따른 어린이집의 원장 또는 보육교사의 자격검정 및 자격증 교부에 관한 사무

「영유아보육법」시행규칙 별지 제11호 및 제12호의2 서식

■ 영유아보호법 시행규칙 [별지 제11호서식] 〈개정 2015.1.28〉

[ ] 어린이집의 원장 / [ ] 보육교사 자격증 [ ] 발급 / [ ] 재발급 신청서

접수번호	접수일	처리기간 14일

신청인	성명	주민등록번호	사진(3cm x 4cm)
	주소		
	전화번호(휴대전화)	전자우편	

■ 영유아보호법 시행규칙 [별지 제12호의 2서식] 〈개정 2011.12.8〉

제 호

( )자 격 증

성 명 :
주민등록번호 :
자 격 :

사 진
3cm x 4cm

25 청소년 상담복지센터 내담자의 주민등록번호 처리

Q **거주하고 있는 시에 설치된 청소년 상담복지센터에 상담을 받으러 갔는데, 주민등록번호를 기재하라고 합니다. 그냥 상담만 받으러 간 것인데 주민등록번호를 알려줘야 하나요?**

A 단순 상담을 위해서는 주민등록번호 처리를 할 수 없습니다. 다만, 상담 이후 복지지원, 긴급구조 등을 위해 불가피한 경우에는 청소년 복지지원법 등에 따라 주민등록번호 처리를 할 수 있습니다.

상세 설명

「청소년복지 지원법」은 법 제29조 제1항에 따라 청소년상담복지센터를 설치하여 다음 기능을 수행하도록 하고 있습니다.

1. 청소년과 부모에 대한 상담·복지지원
2. 상담·복지 프로그램의 개발 및 운영
3. 상담 자원봉사자와 「청소년기본법」 제3조제7호에 따른 청소년지도자에 대한 교육 및 연수
4. 청소년 상담 또는 긴급구조를 위한 전화 운영
5. 청소년 폭력·학대 등으로 피해를 입은 청소년의 긴급구조, 법률 및 의료 지원, 일시 보호 지원
6. 청소년의 자립능력 향상을 위한 자활(自活) 및 재활(再活) 지원
7. 그 밖에 청소년상담 및 복지지원 등을 위하여 필요하다고 특별시장·광역시장·도지사 또는 특별자치도지사가 인정하는 사업

이에 따라 각 시도에 설치된 청소년상담복지센터에는 청소년 전문상담사가 상주하여 청소년에 대한 각종 상담을 수행합니다. 이러한 과정에서 내담자의 주민등록번호 처리가 불가피한 경우에는 주민등록번호를 수집하여 이용할 수 있도록 「청소년복지 지원법」시행령 제18조에 규정되어 있습니다.

그러나 상담의 종류에 따라 학업상담이나 교우관계 상담과 같이 단순한 상담에 그치는 경우에는 주민등록번호를 수집할 불가피성이 반드시 존재하지 않는 경우도 있습니다. 그러므로 전문가 상담이 이루어지는 경우에도 상담의 종류와 내용을 고려하여 내담 청소년의 주민등록번호를 수집하여야 할 불가피성이 있는지를 판단해 보아야 할 것입니다.

관련 법령

「청소년복지 지원법」시행령

제18조(민감정보 및 고유식별정보의 처리) 여성가족부장관 및 지방자치단체의 장(법 제6조제3항 및 제16조제3항에 따라 여성가족부장관 및 지방자치단체의 장의 업무를 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보 및 같은 영 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제4조에 따른 청소년증의 발급 및 재발급 신청과 교부에 관한 업무
2. 법 제6조에 따른 체력검사와 건강진단의 실시, 결과 통보 및 치료 등에 관한 업무
3. 법 제12조에 따른 청소년에 대한 전문가 상담에 관한 사무
4. 법 제13조에 따른 위기청소년의 가족 및 보호자에 대한 상담 및 교육에 관한 사무
5. 법 제14조에 따른 위기청소년 특별지원 및 대상 선정에 관한 사무
6. 법 제16조에 따른 청소년 가출 예방 및 보호·지원에 관한 사무
7. 삭제 〈2015.5.28.〉
8. 법 제18조에 따른 이주배경청소년의 사회 적응 및 학습능력 향상을 위한 상담 및 교육 등에 관한 사무
9. 법 제19조에 따른 교육적 선도 대상자의 선정 및 선도 실시 등에 관한 사무

제 4 장

인사·노무·세무 사례

제4장 인사 · 노무 · 세무 사례

26 기업의 직원 채용시 이력서 · 지원서 등에 주민등록번호 기재

Q **직원을 채용하려 하는 경우 이력서, 지원서 등에 주민등록번호를 기재하도록 하여도 되는지요?**

A 최종합격하여 직원이 되기 전까지는 주민등록번호 수집이 불필요하므로 관련 서식의 기재사항을 생년월일 등으로 대체하여야 합니다.

상세 설명

일반적으로 민간 기업 등의 경우에는 해당 업무별로 적절한 인재를 평가 · 선발하기 위하여 필요한 최소한의 개인정보를 결정하고, 이에 따라 이력서나 지원서 등의 서식을 결정한 후 채용절차를 진행하고 있습니다. 또한 이렇게 결정된 '채용 단계에서의 필요 최소한의 개인정보'를 수집하는 것은 원칙적으로 정보주체의 동의 없이 가능합니다.

그러나 채용전형이 진행 중인 단계에서는 주민등록번호를 반드시 수집 · 이용하여야 할 필요성은 인정되지는 않으며(불가피성 불인정), 또한 인사 · 노무 관계 법령에서 일반적인 채용절차를 위하여 주민등록번호를 반드시 수집 · 이용하도록 하는 근거규정도 존재하지 않습니다(근거규정 부존재). 따라서 기업의 채용진행 단계에서는 이력서, 지원서 등에 주민등록번호 기재항목을 두어서는 아니 되며, 생년월일 정보 등으로 대체하는 것이 바람직합니다. 특히 시중에서 유통 · 활용되는 이력서 양식에는 주민등록번호 기재란이 있는 경우가 많으므로 이런 경우에도 기업의 인사 담당 부서에서는 불필요하게 주민등록번호가 수집되지 않도록 주의를 기울여야 합니다.

〈직원 채용 시 최소한의 개인정보 예시〉
- 지원자 확인 및 연락에 필요한 정보 : 이름, 전화번호, 주소
- 지원자의 직무수행능력을 평가하는데 필요한 정보 : 학력, 성적, 자격사항
  (채용예정 직위의 직무수행을 위해 학력, 경력, 자격이 요구되는 경우)

다만 직원의 채용이 결정된 이후에는 「근로기준법」에 따른 근로계약 체결과 임금대장 작성, 「소득세법」등에 따른 원천징수 처리, 「국민건강보험법」, 「국민연금법」등에 따른 공적보험 처리를 위하여 주민등록번호의 수집 · 이용이 필요하게 됩니다. 따라서 이 경우에는 신규 채용이 결정된 직원으로부터 주민등록번호를 수집 · 이용할 수 있습니다.

참고자료

행정자치부·고용노동부, 「개인정보보호 가이드라인 [인사·노무 편]」, 2015. 12.

27 공무원 임용, 공공기관 채용 지원서에 주민등록번호 기재

Q **공무원 임용이나 공공기관 채용을 위한 지원서 등에 주민등록번호를 기재하도록 하여도 되는 것인지요?**

A 공공기관이라 하더라도 임용이나 채용이 「공무원임용시험령」 제34조 및 「지방공무원 임용령」 제63조에 해당하는 경우와 같이 관련 법령상 근거가 있는 경우에만 지원서 등에 주민등록번호를 기재하도록 할 수 있습니다.

상세 설명

일반직 국가공무원과 외무공무원의 임용시험은 다른 법령에 특별한 규정이 없으면 「공무원임용시험령」에서 정하는 바에 따르고, 「지방공무원법」 제2조에 따른 지방자치단체의 공무원 중 경력직공무원의 임용에 관하여는 다른 법령에 특별한 규정이 없으면 「지방공무원 임용령」에서 정하는 바에 따르게 됩니다.

공무원 임용시험은 직급별로 실시하되, 특수한 직렬에 대해서는 직류별로 분리하여 실시할 수 있으며, 임용 대상자가 「국가공무원법」 제33조(결격사유) 및 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」 제82조(비위면직자의 취업제한)에 해당하는지를 검토하게 됩니다.

「공무원임용시험령」 제34조 제5항은 "시험실시기관의 장은 이 영에 따른 시험 및 채용 사무의 수행을 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보나 같은 법 시행령 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다"고 규정하고 있습니다.

그리고 「지방공무원 임용령」 제63조는 "임용시험 응시자는 시험실시기관의 장이 정하는 응시원서 등을 시험실시기관의 장이 정한 방식에 따라 제출(정보통신망에 의한 제출을 포함한다)하여야 하며 응시원서에 다음 각 호의 사항을 포함한다"고 규정하고 있습니다. 각 호의 사항은 다음과 같습니다.

1. 주민등록번호, 성명, 주소, 사진 등 응시자 본인임을 확인할 수 있는 정보
2. 학력, 자격정보 등 시험이 정하는 응시자격과 관련된 사항
3. 그 밖에 임용시험 응시를 위하여 필요한 사항

따라서 위와 같은 법령에 의거하여 임용되는 공무원의 경우에는 응시원서 등에 주민등록번호를 기재하도록 하는 것이 적법하지만, 이러한 구체적 근거 법령이 없는 경우에는 비록 공공기관의 직원을 채용하는 경우라 하더라도 지원서 등에 주민등록번호를 기재하도록 하면 「개인정보 보호법」 제24조의2에 위배될 것입니다.

28 장애인 우선 채용을 위한 주민등록번호 수집 · 이용

Q **장애인의 우선 채용을 위하여 주민등록번호를 수집 · 이용할 수 있는지요?**

A 장애인의 우선 채용 등은「장애인 고용촉진 및 직업재활법」등의 관련 법령에 구체적인 허용 근거가 있으므로 주민등록번호의 수집 · 이용이 허용됩니다.

상세 설명

기업이나 공공기관 등의 직원을 채용하는 과정에서 관련 법령의 근거에 따라 특정한 신분이나 지위에 있는 사람에게 채용 우대 등을 하는 경우가 있습니다. 가장 대표적인 사례로서 장애인에 대한 채용 우대를 들 수 있습니다.

관련 법령을 살펴보면,「장애인고용촉진 및 직업재활법」에서는 국가와 지방자치단체의 장애인 고용의무(동법 제27조), 상시 50명 이상의 근로자를 고용하는 사업주의 장애인 고용의무(동법 제28조) 등을 규정함으로써 일정 비율 이상의 장애인 채용 우대를 정하고 있습니다. 그런데 국가나 지방자치단체에서 장애인 고용의무를 준수하기 위해서는 당연히 해당 지원자가 장애인인지 여부를 확인하는 것이 필요합니다.

이와 관련하여, 장애인 여부를 확인할 수 있는 '장애인등록증'(복지카드)에는 장애인의 성명, 주소, 사진, 주민등록번호, 장애종류, 장애등급 등을 기재하도록 법령에서 정하고 있습니다(「장애인복지법」시행규칙 제5조).

* 다만 신용카드 기능이 결합된 장애인등록증(복지카드)에는 주민등록번호가 기재되지 않은 경우가 있음

그리고 사업주는 장애인 고용계획 및 실시상황보고서를 제출할 의무가 있는데, 여기에는 장애인의 성명, 주민등록번호 등이 기재된 '장애인 근로자 명부'와 장애인 또는 중증장애인임을 증명할 수 있는 서류 사본을 첨부하여 제출하도록 하고 있습니다(「장애인고용촉진 및 직업재활법」시행규칙 제11조, 별지 제6호 서식).

따라서 장애인의 채용 우대 등을 위하여 해당 장애인의 주민등록번호를 수집 · 이용하는 것은 '법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'에 해당하므로, 이 때에는 장애인의 주민등록번호를 수집 · 이용할 수 있습니다.

관련 법령

「장애인 고용촉진 및 직업재활법」

제11조(장애인 고용계획 등의 제출) ① 영 제27조에 따라 사업주가 전년도 장애인 고용계획에 대한 실시상황과 해당 연도 고용계획을 제출하려면 별지 제6호서식의 장애인 고용계획 및 실시상황 보고서에 다음 각 호의 서류를 첨부하여 공단에 제출하여야 한다.

1. 장애인 근로자 명부 사본 1부
2. 장애인 또는 중증장애인임을 증명할 수 있는 서류 사본 1부(해당 근로자에 대한 최초의 보고 후에는 이 서류의 제출을 생략할 수 있다

「장애인 고용촉진 및 직업재활법」시행규칙 별지 제6호 서식

■장애인고용촉진 및 직업재활법 시행규칙 [별지 제6호서식] <개정 2014.12.31>

전자신고로(전자신청으로)할 수 있습니다.(www.esingo.or.kr)

[ ] 장애인 고용계획 및 실시상황 보고서 **[ ] 장애인 고용장려금 신청서**

[ ] 장애인 고용부담금 신고서 **[ ] 장애인 고용부담금 분할납부 신청서**

[구비서류 양식] 장애인 근로자 명부 <별지 작성>

연번	사업장명	사업자 등록번호	장애인 근로자명	주민등록 번호	장애인정 구분	장애 유형	장애 등급	중증(경증) 여부	중증 2배수 인정여부	장애인정 일	입사일	퇴사일	근무 직무	임금 (원)	「고용보호법」등에 따른 각종 장려금 및 지원금을 지급받은 기간
															-

참고자료

- 행정자치부 · 고용노동부, 「개인정보보호 가이드라인 [인사 · 노무 편]」, 2015. 12.
- 행정자치부 보도자료, "공무원시험에 장애인 차별적 요소 없앤다 - 안행부, 장애인등록증(복지카드) 공무원시험 본인확인용 신분증 인정", 2014. 4. 9.

29 신원조사를 위한 주민등록번호 수집 · 이용

Q **이른바 신원조사를 실시하기 위하여 주민등록번호를 처리할 수 있는지요?**

A 공무원 임용 예정자와 같이 신원조사의 대상이 되는 사람에 대한 신원조사를 실시하기 위하여 주민등록번호를 수집 · 이용할 수 있습니다.

상세 설명

'신원조사'란 국가보안을 위하여 국가에 대한 충성심 · 성실성 및 신뢰성을 조사하기 위하여 시행하는 조사를 의미합니다(「보안업무규정」제33조제1항). 신원조사의 대상이 되는 사람은 다음과 같습니다(「보안업무규정」제33조제3항).

① 공무원 임용 예정자
② 비밀취급 인가 예정자
③ 해외여행을 위하여 「여권법」에 따른 여권이나 「선원법」에 따른 선원수첩 등 신분증서 또는 「출입국관리법」에 따른 사증(査證) 등을 발급받으려는 사람(입국하는 교포를 포함한다)
④ 국가보안시설·보호장비를 관리하는 기관 등의 장(해당 국가보안시설 등의 관리 업무를 수행하는 소속 직원을 포함한다)
⑤ 임직원을 임명할 때 정부의 승인이나 동의가 필요한 공공기관의 임직원
⑥ 그 밖에 다른 법령에서 정하는 사람이나 각급기관의 장이 국가보안상 필요하다고 인정하는 사람

한편, 「보안업무규정」에서는 각급기관의 장은 '신원조사에 관한 사무'를 수행하기 위하여 불가피한 경우에는 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있도록 하는 근거 규정을 두고 있습니다(「보안업무규정」제46조제2호).

* '각급기관'이란 국가기관(군기관 및 교육기관을 포함함), 지방자치단체, 공공기관을 말함(「보안업무규정 제2조제2호)

따라서 국가기관 및 지방자치단체의 공무원 임용 예정자, 공공기관의 임직원, 비밀취급 인가가 필요하거나 국가보안시설 · 보호장비를 관리하는 민간기업 직원 채용 예정자 등에 대한 신원조사를 실시하기 위하여 주민등록번호를 수집 · 이용할 수 있습니다. 또한 「보안업무규정」 외에 다른 법령에서 정하는 사람의 경우에도 신원조사를 실시해야 하는 경우가 있습니다.

* 예를 들어 「항공보안법」 시행규칙 제6조에서는 공항 보호구역등에 대한 출입허가를 위해 신원조사를 실시할 것을 규정하고 있음

관련 법령

「보안업무규정」

제33조(신원조사) ① 국가정보원장은 국가보안을 위하여 국가에 대한 충성심·성실성 및 신뢰성을 조사하기 위하여 신원조사를 한다.

② 신원조사는 국가정보원장이 직권으로 하거나 관계 기관의 장의 요청에 따라 한다.

③ 신원조사의 대상이 되는 사람은 다음 각 호와 같다.

1. 공무원 임용 예정자
2. 비밀취급 인가 예정자
3. 해외여행을 위하여 「여권법」에 따른 여권이나 「선원법」에 따른 선원수첩 등 신분증서 또는 「출입국관리법」에 따른 사증(　　) 등을 발급받으려는 사람(입국하는 교포를 포함한다)
4. 국가보안시설·보호장비를 관리하는 기관 등의 장(해당 국가보안시설 등의 관리 업무를 수행하는 소속 직원을 포함한다)
5. 임직원을 임명할 때 정부의 승인이나 동의가 필요한 공공기관의 임직원
6. 그 밖에 다른 법령에서 정하는 사람이나 각급기관의 장이 국가보안상 필요하다고 인정하는 사람

제46조(고유식별정보의 처리) 각급기관의 장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

2. 제33조에 따른 신원조사에 관한 사무

「보안업무규정」시행규칙 (대통령훈령 제341호)

제58조(신원조사 사항) 신원조사사항에는 다음 각 호의 사항이 포함되어야 한다. 다만, 임용분야 및 취급업무에 따라 신원조사 사항을 생략할 수 있다.

1. 이름 및 주민등록번호 (이하 생략)

「보안업무규정」시행규칙 (대통령훈령 제341호) 별지 제23호 서식

[별지 제23호 서식]

신원조사 회보서

. . . 작성

소 속		직 위		조사목적	
성 명			주민등록번호		
국가관 및 직무자세					
준법성 및 보안의식					

30 채용시 성범죄자 확인을 위한 주민등록번호를 수집 · 이용

Q **학교, 유치원, 학원, 어린이집 등에서 성범죄자의 채용 제한을 위해 주민등록번호를 수집 · 이용할 수 있는지요?**

A 성범죄자는 관련 법령에 따라 아동 · 청소년 관련기관 등에 취업 또는 사실상 노무를 제공할 수 없습니다. 따라서 아동·청소년 관련기관 등에서는 이동 · 청소년의 성보호에 관한 법률에 따라 성범죄자의 취업제한 및 경력조회를 위해 취업희망자의 주민등록번호를 수집·이용할 수 있습니다.

상세 설명

아동 · 청소년이나 성인을 대상으로 성범죄를 저지른 사람에 대해서는 2차적 성범죄 피해의 예방 · 방지를 위하여 일정한 법적 요건 하에서 아동 · 청소년 관련기관 등에 취업을 제한하고 있습니다.

보다 자세한 내용을 살펴보면, 아동 · 청소년 대상 성범죄 또는 성인 대상 성범죄로 형 또는 치료감호를 선고받아 확정된 자(이하 '성범죄자'로 칭함)는 그 형 또는 치료감호의 전부 또는 일부의 집행을 종료하거나 집행이 유예 · 면제된 날로부터 10년 동안 가정을 방문하여 아동 · 청소년에게 직접교육서비스를 제공하는 업무에 종사할 수 없으며, '아동 · 청소년 관련기관 등'을 운영하거나 취업 또는 사실상 노무를 제공할 수 없습니다(「아동 · 청소년의 성보호에 관한 법률」제56조제1항).

〈 아동 · 청소년 관련기관 등의 종류 〉

① 유치원	② 학교	③ 학원, 교습소, 개인과외교습자
④ 청소년 보호·재활센터	⑤ 청소년활동시설	⑥ 청소년상담복지센터, 청소년쉼터
⑦ 어린이집	⑧ 아동복지시설	⑨ 청소년 지원시설, 성매매피해상담소
⑩ 공동주택의 관리사무소		
⑪ 체육시설 중 아동·청소년의 이용이 제한되지 아니하는 체육시설로서 문화체육관광부장관이 지정하는 체육시설		
⑫ 의료기관		
⑬ 인터넷컴퓨터게임시설제공업, 복합유통게임제공업		
⑭ 경비업을 행하는 법인		
⑮ 청소년활동의 기획·주관·운영을 하는 사업장(청소년활동기획업소)		
⑯ 대중문화예술기획업소		
⑰ 청소년게임제공업을 하는 시설 등, 노래연습장업을 하는 시설 등		

이러한 아동 · 청소년 관련기관 등의 장은 그 기관에 취업 중이거나 사실상 노무를 제공 중인 자, 취업하려 하거나 사실상 노무를 제공하려는 자에 대해 성범죄의 경력을 확인할 의무가 있습니다(「아동 · 청소년의 성보호에 관한 법률」제56조제3항). 이 경우 아동 · 청소년 관련기관

등의 장은 취업희망자 본인의 동의를 받아 관계 기관(경찰관서)에 성범죄의 경력 조회를 요청해야 합니다. 이 경우 성범죄 경력조회 신청서 및 성범죄 경력조회 동의서 서식에는 조회 대상자의 성명과 주민등록번호(외국인의 경우에는 외국인등록번호), 연락처 등을 기재하도록 하고 있습니다(「아동·청소년의 성보호에 관한 법률」시행규칙 별지 제9호 및 제10호 서식).

따라서 아동 · 청소년 관련기관 등에서 성범죄자의 채용 제한을 위하여 취업 희망자의 주민등록번호를 수집·이용하는 것은 '법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'에 해당하므로, 이 때에는 취업 희망자의 주민등록번호를 수집 · 이용하는 것이 허용됩니다.

관련 법령

「아동·청소년의 성보호에 관한 법률」

제56조(아동·청소년 관련기관 등에의 취업제한 등) ① 아동·청소년대상 성범죄 또는 성인대상 성범죄(이하 "성범죄"라 한다)로 형 또는 치료감호를 선고받아 확정된 자(제11조제5항에 따라 벌금형을 선고받은 자는 제외한다)는 그 형 또는 치료감호의 전부 또는 일부의 집행을 종료하거나 집행이 유예·면제된 날부터 10년 동안 가정을 방문하여 아동·청소년에게 직접교육서비스를 제공하는 업무에 종사할 수 없으며 다음 각 호에 따른 시설·기관 또는 사업장(이하 "아동·청소년 관련기관 등"이라 한다)을 운영하거나 아동·청소년 관련기관 등에 취업 또는 사실상 노무를 제공할 수 없다. 다만, 제10호 및 제14호 경우에는 경비업무에 종사하는 사람, 제12호의 경우에는 「의료법」 제2조의 의료인에 한한다. (이하 각 호 생략)

③ 아동·청소년 관련기관 등의 장은 그 기관에 취업 중이거나 사실상 노무를 제공 중인 자 또는 취업하려 하거나 사실상 노무를 제공하려는 자에 대하여 성범죄의 경력을 확인하여야 한다. 이 경우 본인의 동의를 받아 관계 기관의 장에게 성범죄의 경력 조회를 요청하여야 한다.

「아동·청소년의 성보호에 관한 법률」시행령

제25조(성범죄의 경력 조회) ① 법 제56조제2항 및 제3항에 따라 성범죄의 경력조회를 요청하려는 지방자치단체의 장, 교육감, 교육장 또는 법 제56조제1항 각 호에 따른 시설 · 기관 또는 사업장(이하 "아동 · 청소년 관련기관 등"이라 한다)의 장은 경찰관서의 장에게 요청하여야 한다. 이 경우 경찰관서가 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망(이하 "정보통신망"이라 한다)을 이용하여 요청할 수 있다.

② 아동 · 청소년 관련기관 등의 장은 제1항에 따라 성범죄의 경력 조회를 요청하는 경우 취업 중이거나 사실상 노무를 제공 중인 사람(이하 "취업자"라 한다) 또는 취업하려 하거나 사실상 노무를 제공하려는 사람(이하 "취업예정자"라 한다)의 동의서를 함께 제출하거나, 경찰관서가 운영하는 정보통신망에 취업자나 취업예정자가 동의 여부를 표시하도록 하여야 한다.

「아동·청소년의 성보호에 관한 법률」시행규칙 별지 제9호 및 제10호 서식

■ 아동·청소년의 성보호에 관한 법률 시행규칙 [별지 제9호서식] <개정 2015.5.1>

성범죄 경력조회 신청서

접수번호		접수일자	처리일자	처리기간 즉시
신청인	성명		주민등록번호	
	기관명			
	주소		(전화번호:)	
대상자	성명			
	주민등록번호(외국인의 경우 생년월일)		외국인등록번호(외국인의 경우만 기입)	

■ 아동·청소년의 성보호에 관한 법률 시행규칙 [별지 제10호서식] <개정 2015.5.1>

성범죄 경력 조회 동의서

대상자	성명(외국인의 경우 영문으로 작성)	
	주민등록번호(외국인의 경우 생년월일)	외국인등록번호(외국인의 경우만 기입)
	연락처(휴대전화 등)	

참고자료

- 행정자치부 · 고용노동부, 「개인정보보호 가이드라인 [인사 · 노무 편]」, 2015. 12.
- 여성가족부 보도자료, "성범죄경력 조회절차 간소화", 2014. 10. 21.

31 직원 인사기록에 주민등록번호 보유

Q **저희 기업에서는 직원의 인사기록에 주민등록번호를 보유하고 있습니다. 주민등록번호 처리가 전면 금지되었다고 하는데 문제가 되는 것 아닌지요?**

A 기업이 소속 직원의 인사 · 급여 기록 등에 주민등록번호를 수집 · 보유하는 것은 관련 법령에 구체적 근거가 마련되어 있으므로 허용됩니다.

상세 설명

기업이나 공공기관 등이 소속 직원의 인사·급여 업무를 위하여 주민등록번호를 수집 · 이용 · 보관하는 것에 대해서는 다양한 관계법령에 그 근거가 마련되어 있으며, 또한 주민등록번호 처리의 불가피성이 인정되고 있습니다.

우선 「근로기준법」제48조는 사용자가 임금대장을 작성하도록 의무화하고 있으며, 동법 시행령 제27조는 임금대장의 기재사항으로서 근로자의 성명, 주민등록번호, 고용 연월일, 종사업무, 임금 및 가족수당의 계산기초가 되는 사항 등을 기재하도록 하고 있습니다.

「소득세법」제127조는 원천징수의무자로 하여금 근로소득 등에 대한 원천징수의무를 규정하고 있으며, 동법 시행규칙 별지 제37호 서식(소득 · 세액 공제신고서/근로소득자 소득 · 세액 공제신고서) 등은 근로소득 원천징수 처리를 위해 주민등록번호를 기재하도록 명시하고 있습니다.

이 외에 「국민연금법」, 「국민건강보험법」, 「고용보험법」, 「산업재해보상보험법」등 이른바 4대 공적보험의 가입 등 제반업무를 수행하기 위한 주민등록번호 처리 근거규정도 마련되어 있습니다.

결론적으로, 기업(고용주, 사용자 등)은 소속 직원의 인사 · 급여 · 4대보험 등의 처리를 위하여, 주민등록번호 처리금지 원칙에도 불구하고 관련 법령에 구체적 근거규정이 마련되어 있으므로 주민등록번호를 수집 · 이용 · 보관할 수 있습니다.

관련 법령

「근로기준법」

제48조(임금대장) 사용자는 각 사업장별로 임금대장을 작성하고 임금과 가족수당 계산의 기초가 되는 사항, 임금액, 그 밖에 대통령령으로 정하는 사항을 임금을 지급할 때마다 적어야 한다.

「근로기준법」시행령

제27조(임금대장의 기재사항) ① 사용자는 법 제48조에 따른 임금대장에 다음 각 호의 사항을 근로자 개인별로 적어야 한다.

1. 성명
2. 주민등록번호 (이하 생략)

「소득세법」

제127조(원천징수의무) ① 국내에서 거주자나 비거주자에게 다음 각 호의 어느 하나에 해당하는 소득을 지급하는 자(제3호의 소득을 지급하는 자의 경우에는 사업자 등 대통령령으로 정하는 자로 한정한다)는 이 절의 규정에 따라 그 거주자나 비거주자에 대한 소득세를 원천징수하여야 한다.

1. 이자소득
2. 배당소득
3. 대통령령으로 정하는 사업소득(이하 "원천징수대상 사업소득"이라 한다)
4. 근로소득 (이하 생략)

「소득세법」시행규칙 서식 제37호

(8쪽 중 제1쪽)

소득·세액 공제신고서/근로소득자 소득·세액 공제신고서(　　년 소득에 대한 연말정산용)

※ 근로소득자는 신고시에 소득·세액 공제서류를 첨부하여 원천징수의무자(소속회사 등)에게 제출하며, 원천징수의무자는 신고서 및 첨부서류를 확인하여 근로소득 세액계산을 하고 근로소득자에게 즉시 근로소득원천징수영수증을 발급해야 합니다. 연말정산 시 근로소득자에게 환급이 발생하는 경우 원천징수의무자는 근로소득자에게 환급세액을 지급해야 합니다.

소득자 설명		주민등록번호	-
근무처 명칭		사업자등록번호	- -
세대주 여부	[ ] 세대주 [ ]세대원	국 적	(국적코드 :)
근무기간		감면기간	~
거주구분	[ ] 거주자 [ ]비거주자	거주지국	(거주지국 코드 :)
인적공제 항목 변동여부	[ ] 전년과 동일 [ ]변동	※ 인적공제 항목이 전년과 동일한 경우에는 주민등록표등본을 제출하지 않습니다.	

「국민연금법」시행규칙 서식 제6호

국민연금 [ ] 사업장가입자자격취득신고서　　건강보험 [ ] 직장가입자자격취득신고서
고용보험 [ ] 피보험자격취득신고서　　산재보험 [ ] 근로자고용신고서

※ 유의사항 및 작성방법은 제1쪽 뒷면을 참고하여 주시기 바라며, 색상이 어두운 란은 신청인이 적지 않습니다.　　(제1쪽앞면)

접수번호	접수일	처리기간	3일(고용보험은 5일)

사업장	사업장관리번호		명칭	단위사업장명칭	영업소명칭
	소재지				우편번호(-)
	전화번호	(유선)	(이동전화)	FAX번호	
보험사무대행 기관	번호		명칭	하수급인 관련번호(건설공사 등의 미승인 하수급인만 해당함)	

	성명	국적	대표자여부	[ ]국민연금([ ]취득 월 납부 희망)					[ ] 건강보험						[ ] 고용보험(계약직 여부 : [ ]예, [ ]아니오) [ ] 산재보험						
	주민(외국인)등록번호	체류자격	[ ]예 [ ]아니오	소득월액(원)	자격취득부호	자격취득일	특수직종부호	직역연금부호	보수월액(원)	자격취득부호	자격취득일	보험료 감면부호	공무원 회계명/부호	교직원 직종명/부호	월평균보수	학력	직종	자격취득일	주소정근로시간	계약종료연월일(계약직 만작성)	비고
1																					

32 퇴사한 직원의 주민등록번호 보관

Q **근로자가 퇴직한 이후에 주민등록번호를 보관할 수 있는지요? 만약 보관해야 한다면 어느 정도의 기간 동안 보관해야 하는지요?**

A 근로자가 퇴직한 이후에는 근로자의 개인정보를 파기하는 것이 원칙이나 국세기본법 등에 따라 입금관련 기록을 보관하여야 하며 이를 위해 주민등록번호를 보관하여야 합니다.(5년)

상세 설명

기업 등 사용자는 근로자가 퇴직한 이후, 개인정보 보호법에 따라 퇴직자의 개인정보를 삭제하는 것이 원칙입니다. 다만, 국세기본법 등에는 납세와 관련된 정보와 함께 주민등록번호를 보관하도록 하고 있습니다. 따라서 기존 인사정보와 분리하여 해당 정보를 보관하여야 할 것입니다.

* 「국세기본법」 제85조의3은 납세자로 하여금 모든 거래에 관한 장부 및 증거서류 등의 작성·비치 및 해당 국세 법정신고기한이 지난 날부터 5년간 보존의무를 규정하고 있으며, 「소득세법」 및 동법 시행령·시행규칙 상의 주요 서식에서는 납세자의 주민등록번호 기재를 규정하고 있는 바, 근로자의 임금에 대한 소득세의 원천징수 관련 내역(주민등록번호 포함) 등은 임금대장과 연계하여 5년간 보존의무가 있는 것입니다.

관련 법령

「개인정보보호법 제21조」

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

관련 법령

「근로기준법」

제39조(사용증명서) ① 사용자는 근로자가 퇴직한 후라도 사용 기간, 업무 종류, 지위와 임금, 그 밖에 필요한 사항에 관한 증명서를 청구하면 사실대로 적은 증명서를 즉시 내주어야 한다.

② 제1항의 증명서에는 근로자가 요구한 사항만을 적어야 한다.

제42조(계약 서류의 보존) 사용자는 근로자 명부와 대통령령으로 정하는 근로계약에 관한 중요한 서류를 3년간 보존하여야 한다.

제48조(임금대장) 사용자는 각 사업장별로 임금대장을 작성하고 임금과 가족수당 계산의 기초가 되는 사항, 임금액, 그 밖에 대통령령으로 정하는 사항을 임금을 지급할 때마다 적어야 한다.

「근로기준법」시행령

제19조(사용증명서의 청구) 법 제39조제1항에 따라 사용증명서를 청구할 수 있는 자는 계속하여 30일 이상 근무한 근로자로 하되, 청구할 수 있는 기한은 퇴직 후 3년 이내로 한다.

제20조(근로자 명부의 기재사항) 법 제41조제1항에 따른 근로자 명부에는 고용노동부령으로 정하는 바에 따라 다음 각 호의 사항을 적어야 한다.

1. 성명
2. 성( )별
3. 생년월일
4. 주소
5. 이력( )
6. 종사하는 업무의 종류
7. 고용 또는 고용갱신 연월일, 계약기간을 정한 경우에는 그 기간, 그 밖의 고용에 관한 사항
8. 해고, 퇴직 또는 사망한 경우에는 그 연월일과 사유
9. 그 밖에 필요한 사항

제22조(보존 대상 서류 등) ① 법 제42조에서 "대통령령으로 정하는 근로계약에 관한 중요한 서류"란 다음 각 호의 서류를 말한다.

1. 근로계약서
2. 임금대장
3. 임금의 결정·지급방법과 임금계산의 기초에 관한 서류
4. 고용·해고·퇴직에 관한 서류
5. 승급·감급에 관한 서류
6. 휴가에 관한 서류
7. 삭제 〈2014.12.9.〉
8. 법 제51조제2항, 법 제52조, 법 제58조제2항·제3항 및 법 제59조에 따른 서면 합의

서류

9. 법 제66조에 따른 연소자의 증명에 관한 서류

② 법 제42조에 따른 근로계약에 관한 중요한 서류의 보존기간은 다음 각 호에 해당하는 날부터 기산한다.

1. 근로자 명부는 근로자가 해고되거나 퇴직 또는 사망한 날
2. 근로계약서는 근로관계가 끝난 날
3. 임금대장은 마지막으로 써 넣은 날
4. 고용, 해고 또는 퇴직에 관한 서류는 근로자가 해고되거나 퇴직한 날
5. 제1항제7호의 승인이나 인가에 관한 서류는 승인이나 인가를 받은 날
6. 제1항제8호의 서면 합의 서류는 서면 합의한 날
7. 연소자의 증명에 관한 서류는 18세가 되는 날(18세가 되기 전에 해고되거나 퇴직 또는 사망한 경우에는 그 해고되거나 퇴직 또는 사망한 날)
8. 그 밖의 서류는 완결한 날

제27조(임금대장의 기재사항) ① 사용자는 법 제48조에 따른 임금대장에 다음 각 호의 사항을 근로자 개인별로 적어야 한다.

1. 성명
2. 주민등록번호 (이하 생략)

33 사용증명서(재직증명서, 경력증명서 등)에 주민등록번호 기재

Q **퇴직자가 재직증명서나 경력증명서 등을 요구하는 경우에 주민등록번호를 기재하여 발급해도 되는지요?**

A 퇴직자에 대한 사용증명서에는 주민등록번호를 기재하여서는 안 됩니다. 다만 다른 법령에 따른 확인 목적으로 사용증명서를 발급하는 경우에는 예외가 있을 수 있습니다.

상세 설명

기업 등의 사용자는 근로자가 퇴직한 후라도 사용 기간, 업무 종류, 지위와 임금, 그 밖에 필요한 사항에 관한 사용증명서를 청구하면 사실대로 적은 증명서를 즉시 내주어야 할 의무가 있습니다. 그리고 사용증명서에는 근로자가 요구한 사항만을 적어야 합니다(「근로기준법」제39조). 사용증명서를 청구할 수 있는 자는 계속하여 30일 이상 근무한 근로자이며, 청구할 수 있는 기한은 퇴직 후 3년 이내입니다(「근로기준법」제39조제1항, 동법 시행령 제19조). 이상의 내용을 볼 때, 「근로기준법」에는 사용증명서에 주민등록번호를 기재하도록 한 명시적인 근거 규정이 존재하지 않으므로, 원칙적으로 사용증명서에는 주민등록번호를 기재하여 발급하여서는 아니됩니다.

관련 법령

「근로기준법」

제39조(사용증명서) ① 사용자는 근로자가 퇴직한 후라도 사용 기간, 업무 종류, 지위와 임금, 그 밖에 필요한 사항에 관한 증명서를 청구하면 사실대로 적은 증명서를 즉시 내주어야 한다.

② 제1항의 증명서에는 근로자가 요구한 사항만을 적어야 한다.

「근로기준법」시행령

제19조(사용증명서의 청구) 법 제39조제1항에 따라 사용증명서를 청구할 수 있는 자는 계속하여 30일 이상 근무한 근로자로 하되, 청구할 수 있는 기한은 퇴직 후 3년 이내로 한다.

34 자문료 등 수당 지급을 위한 주민등록번호 처리

Q **외부인에 대한 강사료, 자문료, 수당 등을 지급하기 위해 주민등록번호를 수집 · 이용할 수 있는지요?**

A 강사료, 자문료, 수당 등 이른바 '기타소득'을 위한 주민등록번호 수집 · 이용은 「소득세법」 등 관련 법령에 구체적인 근거가 있으므로 허용됩니다.

상세 설명

'기타소득'이란 이자소득 · 배당소득 · 사업소득 · 근로소득 · 연금소득 · 퇴직소득 및 양도소득 외의 소득을 말합니다. 여기에는 원고료, 인세, 사례금, 강연료(고용관계 없이 다수인에게 강연을 하고 받는 대가), 변호사 등의 전문적 지식 또는 특별한 기능을 가진 자가 그 지식 또는 기능을 활용하여 제공하는 용역에 대한 보수, 기타 고용관계 없이 제공하는 용역에 대한 수당 또는 이와 유사한 성질의 대가 등이 포함됩니다(「소득세법」 제21조제1항). 따라서 기업이나 공공기관 등이 고용관계가 없는 외부인에 대해 지급하는 강사료, 자문료, 원고료, 각종 수당 등은 「소득세법」에 따른 '기타소득'에 해당합니다.

한편 「소득세법」은 원천징수의무자로 하여금 기타소득에 대한 원천징수 처리 및 원천징수영수증 발급(「소득세법」 제145조), 관할 세무서 등에 대한 지급명세서 제출(「소득세법법」 제164조) 등을 규정하고 있습니다. 이에 더하여 「소득세법」 시행규칙은 기타소득에 대한 원천징수영수증 서식, 지급명세서 서식 등을 정하여 두고 있으며 여기에는 기타소득 소득자의 성명, 주민등록번호, 주소 등을 기재하도록 하고 있습니다.

따라서 공공기관이나 기업 등의 원천징수의무자가 기타소득에 대한 원천징수 등 제반 처리를 하기 위하여 소득자(즉 외부 전문가, 외부 강사 등)로부터 주민등록번호를 수집 · 이용하는 것은 관련 법령에서 구체적으로 주민등록번호의 처리를 요구 · 허용한 경우에 해당하고, 또한 소득자의 정확한 식별을 위한 불가피성도 인정될 수 있으므로, 결론적으로 강사료, 자문료, 수당 등 기타소득 처리를 위한 주민등록번호 수집 · 이용은 허용됩니다.

관련 법령

「소득세법」

제145조(기타소득에 대한 원천징수시기와 방법 및 원천징수영수증의 발급) ① 원천징수의무자가 기타소득을 지급할 때에는 그 기타소득금액에 원천징수세율을 적용하여 계산한 소득세를 원천징수한다.

② 기타소득을 지급하는 원천징수의무자는 이를 지급할 때에 그 기타소득의 금액과 그 밖에 필요한 사항을 적은 기획재정부령으로 정하는 원천징수영수증을 그 소득을 받는 사람에게 발급하여야 한다. 다만, 제21조제1항제15호가목 및 제19호가목·나목에 해당하는 기타소득으로서 대통령령으로 정하는 금액 이하를 지급할 때에는 지급받는 자가 원천징수영수증의 발급을 요구하는 경우 외에는 발급하지 아니할 수 있다.

제164조(지급명세서의 제출) ① 제2조에 따라 소득세 납세의무가 있는 개인에게 다음 각 호의 어느 하나에 해당하는 소득을 국내에서 지급하는 자(법인, 제127조제5항에 따라 소득의 지급을 대리하거나 그 지급 권한을 위임 또는 위탁받은 자 및 제150조에 따른 납세조합, 제7조 또는 「법인세법」 제9조에 따라 원천징수세액의 납세지를 본점 또는 주사무소의 소재지로 하는 자와 「부가가치세법」 제8조제3항 후단에 따른 사업자 단위 과세 사업자를 포함한다)는 대통령령으로 정하는 바에 따라 지급명세서를 그 지급일(제131조, 제135조, 제144조의5 또는 제147조를 적용받는 소득에 대해서는 해당 소득에 대한 과세기간 종료일을 말한다. 이하 이 항에서 같다)이 속하는 과세기간의 다음 연도 2월 말일(제3호에 따른 사업소득과 제4호에 따른 근로소득 또는 퇴직소득 및 제7호에 따른 봉사료의 경우에는 다음 연도 3월 10일, 휴업 또는 폐업한 경우에는 휴업일 또는 폐업일이 속하는 달의 다음다음 달 말일)까지 원천징수 관할 세무서장, 지방국세청장 또는 국세청장에게 제출하여야 한다. 다만, 제4호의 근로소득 중 대통령령으로 정하는 일용근로자의 근로소득의 경우에는 그 지급일이 속하는 분기의 마지막 달의 다음 달 말일(4분기에 지급한 근로소득은 다음 과세기간 2월 말일)까지 지급명세서를 제출하여야 한다.

(4쪽 중 제4쪽)

6. 기타소득(제7호에 따른 봉사료는 제외한다)

소득 연도	

소득자 구분	
내·외국인구분	내국인 1 외국인 9

「소득세법」시행규칙 별지 제23호 서식

[ ] 거주자의 기타소득 원천징수영수증
[ ] 거주자의 기타소득 지급 명세서

([ ] 소득자보관용 [ ] 발행자 보관용)

징수 의무자	① 사업자등록번호	② 법인명 또는 상호	③ 성명
	④ 주민(법인) 등록번호	⑤ 소재지 또는 주소	
소득자	⑥ 성명	⑦ 주민(사업자)등록번호	
	⑧ 주소		

⑨소득구분코드 *해당코드에 √표시	63 비과세 기타소득, 69 분리과세 기타소득, 64 소기업소상공인 공제부금 해지 소득, 60 필요경비 없는 기타소득(61 ~ 63 제외), 61 주식매수선택권 행사이익, 62 서화·골동품 양도소득 71 상금 및 부상, 72 광업권 등, 73 지역권 등, 74 주택입주지체상금 75 원고료 등, 76 강연료 등 82 그 밖에 필요경비 있는 기타소득(64 · 66 · 69 · 71 ~ 76 제외)

35 기부금영수증 발급을 위한 주민등록번호 수집 · 이용

Q **사회복지단체에서 기부금영수증을 발급하기 위하여 주민등록번호를 수집 · 이용할 수 있는지요? 만약 가능하다면 기부금 영수증 발급을 위한 주민등록번호는 언제까지 보관할 수 있습니까?**

A 기부금 영수증 발급 및 발급명세 보존 등을 위한 주민등록번호 처리는 「소득세법」등 관련 법령에 근거가 마련되어 있으므로 허용됩니다. 기부금 영수증 발급 등을 위한 주민등록번호는 5년간 보관 의무가 있습니다.

상세 설명

개인이나 사업자가 사회복지, 문화, 예술, 교육, 종교, 자선 등 공익성을 고려하여 지출하는 금액 등을 기부금이라고 부릅니다. 「소득세법」은 기부금을 지출한 사업자에 대해서는 사업소득금액을 계산할 때 필요경비에 산입하지 않고(「소득세법」제34조), 거주자(개인)가 지출한 기부금에 대해서는 종합소득산출세액에서 공제하는 등(「소득세법」제59조의4) 공익성을 위하여 지출한 기부금에 대해서 일정한 혜택을 부과하고 있습니다.

한편, 「소득세법」은 법령상의 기부금 혜택을 악용하는 것을 방지하기 위하여, 기부금 세액공제를 받기 위하여 필요한 기부금영수증을 발급하도록 하는 한편, 기부자별 발급명세를 작성하여 보관하도록 하고, 이를 관할 세무서장에게 제출하도록 의무화하고 있습니다(「소득세법」제160조의3). 또한 기부금액을 사실과 다르게 적어 발급하거나 기부자의 인적 사항 등을 사실과 다르게 적어 발급하는 행위 및 기부금발급명세를 작성 · 보관하지 아니한 경우에 대해서는 가산세를 부과하는 등 제재를 과하고 있습니다(「소득세법」제81조). 특히 기부금영수증 서식 및 기부금영수증 발급명세 서식에서는 기부자의 신원을 명확히 하기 위하여 기부자의 성명, 주민등록번호, 주소 등을 반드시 기재하도록 하고 있습니다.

따라서 기부를 받는 사회복지단체, 종교단체 등에서 기부자들에게 기부금영수증을 발급하는 등 법령에 따른 제반 업무를 처리하기 위해서는 주민등록번호가 반드시 필요하므로, 이 경우에는 해당 기부자의 주민등록번호를 수집 · 이용하는 것은 물론 관할 세무서장에게 제출하는 등의 행위가 허용됩니다. 다만, 기부금영수증 발급을 원하지 않는 경우에는 주민등록번호 처리가 허용되지 아니합니다.

그리고 기부자의 주민등록번호 등이 기재된 '기부금영수증 발급명세'는 기부금 영수증을 발급한 날부터 5년간 보관하여야 할 의무가 있으므로(「소득세법」제160조의3) 이 기간 동안은 당연히 주민등록번호를 보관하여야 한다고 해석될 것입니다.

관련 법령

「소득세법」

제160조의3(기부금영수증 발급명세의 작성 · 보관의무 등) ① 거주자 또는 제121조제2항 및 제5항에 따른 비거주자에게 제34조 또는 제59조의4제4항에 따라 필요경비 산입 또는 기부금세액공제를 받거나 내국법인이 「법인세법」 제24조에 따라 손금에 산입하기 위하여 필요한 기부금영수증을 발급하는 거주자 또는 비거주자(이하 이 조에서 "기부금 영수증을 발급하는 자"로 한다)는 대통령령으로 정하는 기부자별 발급명세를 작성하여 발급한 날부터 5년간 보관하여야 한다.

② 기부금영수증을 발급하는 자는 제1항에 따라 보관하고 있는 기부자별 발급명세를 국세청장, 지방국세청장 또는 관할 세무서장이 요청하는 경우 제출하여야 한다.

③ 기부금영수증을 발급하는 자는 해당 과세기간의 기부금영수증 총 발급 건수 및 금액 등을 기재한 기부금영수증 발급명세서를 해당 과세기간의 다음 연도 6월 30일까지 제168조제5항에 따른 관할 세무서장에게 제출하여야 한다.

「소득세법」시행규칙 별지 제29호의7 서식 (기부금영수증 발급명세)

[별지 제29호의7서식(1)] <개정 2008.4.29>

기부금영수증 발급명세

귀속연도		단 체 명	
		사업자등록번호	

기부자별 발급명세

① 일련번호	② 기부일자	③ 기부자명	④ 주민등록번호(사업자등록번호)	기부내역			발급명세	
		⑤ 주소(사업장)		⑥ 내용	⑦ 코드	⑧ 금액	⑨ 발급번호	⑩ 발급일자

「소득세법」시행규칙 별지 제45호의2 서식 (기부금영수증)

■ 소득세법 시행규칙 [별지 제45호의2서식] <개정 2014.3.14>

일련번호	

기부금 영수증

※ 아래의 작성방법을 읽고 작성하여 주시기 바랍니다.

❶ 기부자

성명(법인명)	주민등록번호 (사업자등록번호)
주소(소재지)	

제 5 장

의료·보건 사례

제5장 의료 · 보건 사례

36 병원 진료 · 검사 예약 위한 주민등록번호 이용

Q **전화나 인터넷 등을 이용하여 진료 · 검사 예약을 하는 경우에 해당 환자의 주민등록번호를 받을 수 있는지요?**

A 병원에 대해 진료 · 검사 예약을 하는 경우에는 건강보험 가입여부, 건강검진 대상여부 등의 확인이 필요하므로 국민건강보험법 등에 따라 주민등록번호의 수집 · 이용이 허용됩니다.

상세 설명

병원 등 의료기관에서 전화나 인터넷 등을 통하여 진료 · 검사 예약을 받는 경우에는 해당 환자나 내원자의 건강보험 가입여부, 건강검진 대상 여부 등 일정 사항의 확인이 요구되므로 이에 필요한 최소한의 개인정보를 수집할 필요가 있습니다. 따라서 이러한 경우에는 「국민건강보험법」 등에 따라 주민등록번호의 수집 · 이용이 가능한 것으로 해석됩니다.

다만 단순한 진료예약(시간약속 등)을 위한 주민등록번호 수집은 원칙적으로 허용되지 아니합니다.

〈인터넷 · 전화 등에 의한 진료 예약 시 수집할 수 있는 개인정보〉

① 성명	④ 연락처
② 주민등록번호	⑤ 진료과목
③ 주소	

한편 인터넷으로 수집한 주민등록번호는 반드시 암호화하여 보관하여야 하며, 팩스 등 문서로 수집된 주민등록번호를 포함한 개인정보도 안전하게 보관 · 관리하여야 합니다. 또한 이를 취급할 수 있는 '개인정보취급자'를 최소하하여 해당 정보를 취급하도록 하여야 합니다.

관련 법령

「국민건강보험법」시행령

제81조(민감정보 및 고유식별정보의 처리) ① 공단(법 제112조에 따라 공단의 업무를 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조 각 호에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

2. 법 제14조제1항에 따른 업무에 관한 사무

「의료법」

제22조(진료기록부 등) ① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 갖추어 두고 환자의 주된 증상, 진단 및 치료 내용 등 보건복지부령으로 정하는 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다.

참고자료

- 보건복지부·행정자치부, 「개인정보보호 가이드라인 [의료기관 편]」, 2015. 2.
- 보건복지부 보도참고자료, “병원 내 진료 · 검사 예약시, 건강보험 자격 등 확인을 위해 필요한 경우 주민등록번호 수집 가능해진다”, 2014. 11. 28.

37 환자의 친족 · 대리인의 의료기록 열람 청구 시 주민등록번호 수집 · 이용

Q **병원에서 환자의 배우자 등 친족이나 대리인이 환자의 의료기록을 대신 요청하는 경우가 있습니다. 이 경우 환자의 친족이나 대리인의 진위여부 확인을 위해 주민등록번호를 수집 · 이용할 수 있는지요?**

A 환자의 친족이나 대리인이 환자의 의료기록을 청구하는 경우에는 친족관계 또는 대리권의 확인을 위하여 환자 본인의 동의서 및 위임장, 열람을 청구하는 자의 신분증, 친족관계임을 확인할 수 있는 서류 등의 법적 요건을 갖추어야 합니다. 따라서 이를 처리하기 위한 범위 내에서는 주민등록번호 수집 · 이용이 허용됩니다.

상세 설명

의료인 · 의료기관은 원칙적으로 환자 본인이 아닌 다른 사람에게 환자에 관한 의료기록을 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있게 하여서는 안됩니다. 다만 일정한 법적 요건을 갖추어 요청하는 경우에는 예외적으로 환자가 아닌 다른 사람에 대해 의료기록 열람이나 사본 교부를 할 수 있습니다(「의료법」제21조).

환자의 친족(환자의 배우자, 직계 존속 · 비속, 배우자의 직계 존속)이 요청하는 때에는

1) 의료기록 열람이나 사본 발급을 요청하는 자의 신분증(주민등록증 등) 사본,

2) 가족관계증명서 · 주민등록표 등본 등 친족관계임을 확인할 수 있는 서류,

3) 환자가 자필 서명한 동의서(「의료법」시행규칙 별지 제9호의2 서식)

4) 환자의 신분증 사본(다만, 환자가 만 17세 미만으로 주민등록증이 발급되지 아니한 자는 제외)을 갖추어 요청하는 경우에 한해 의료기록의 열람 · 사본교부가 가능합니다(「의료법」시행규칙 제13조의2제1항).

환자가 지정하는 대리인이 요청하는 때에는

1) 의료기록 열람이나 사본 발급을 요청하는 자의 신분증(주민등록증 등) 사본,

2) 환자가 자필 서명한 동의서(「의료법」시행규칙 별지 제9호의2 서식) 및 위임장((「의료법」시행규칙 별지 제9호의3 서식),

3) 환자의 신분증 사본(다만, 환자가 만 17세 미만으로 주민등록증이 발급되지 아니한 자는 제외)을 갖추어 요청하는 경우에 한해 의료기록의 열람 · 사본교부가 가능합니다(「의료법」시행규칙 제13조의2제2항).

따라서 신분증 사본, 친족관계임을 확인할 수 있는 서류 등에 기재된 주민등록번호를 수집 ·

이용하는 것은 「의료법」등 관련 법령에 근거가 있는 경우에 해당하므로 그 범위 내에서는 주민등록번호의 수집 · 이용이 허용된다고 해석됩니다.

다만 주의할 점은, 「의료법」시행규칙에 따른 동의서 및 위임장 서식을 살펴보면 이전에는 환자 본인이나 신청인 · 위임인의 주민등록번호를 기재하도록 하였으나, 최근의 시행규칙 개정에 따라 현재는 생년월일(외국인의 경우에는 외국인등록번호)을 기재하도록 하고 있습니다. 따라서 의료기관에서는 동의서나 위임장에 주민등록번호가 기재되지 않도록 주의를 기울여야 하겠습니다.

관련 법령

「의료법」시행규칙

제13조의2(기록 열람 등의 요건) ① 법 제21조제2항제1호에 따라 환자의 배우자, 직계존속·비속 또는 배우자의 직계 존속(이하 이 조에서 "친족"이라 한다)이 환자에 관한 기록의 열람이나 그 사본의 발급을 요청할 경우에는 다음 각 호의 서류를 갖추어 의료기관 개설자에게 제출하여야 한다.

1. 기록 열람이나 사본 발급을 요청하는 자의 신분증(주민등록증, 여권, 운전면허증 그 밖에 공공기관에서 발행한 본인임을 확인할 수 있는 신분증을 말한다. 이하 이 조에서 같다) 사본
2. 가족관계증명서, 주민등록표 등본 등 친족관계임을 확인할 수 있는 서류
3. 환자가 자필서명한 별지 제9호의2서식의 동의서. 다만, 환자가 만 14세 미만의 미성년자인 경우에는 제외한다.
4. 환자의 신분증 사본. 다만, 환자가 만 17세 미만으로 「주민등록법」 제24조제1항에 따른 주민등록증이 발급되지 아니한 경우에는 제외한다.

② 법 제21조제2항제2호에 따라 환자가 지정하는 대리인이 환자에 관한 기록의 열람이나 그 사본의 발급을 요청할 경우에는 다음 각 호의 서류를 갖추어 의료기관 개설자에게 제출하여야 한다.

1. 기록열람이나 사본발급을 요청하는 자의 신분증 사본
2. 환자가 자필 서명한 별지 제9호의2서식의 동의서 및 별지 제9호의3서식의 위임장. 이 경우 환자가 만 14세 미만의 미성년자인 경우에는 환자의 법정대리인이 작성하여야 하며, 가족관계증명서 등 법정대리인임을 확인할 수 있는 서류를 첨부하여야 한다.
3. 환자의 신분증 사본. 다만, 환자가 만 17세 미만으로 「주민등록법」 제24조제1항에 따른 주민등록증이 발급되지 아니한 자는 제외한다.

③ 법 제21조제2항제3호에 따라 환자의 동의를 받을 수 없는 상황에서 환자의 친족이 환자에 관한 기록의 열람이나 그 사본 발급을 요청할 경우에는 별표 2의2에서 정하는 바에 따라 서류를 갖추어 의료기관 개설자에게 제출하여야 한다.

④ 환자가 본인에 관한 진료기록 등을 열람하거나 그 사본의 발급을 원하는 경우에는 본인임을 확인할 수 있는 신분증을 의료기관 개설자에게 제시하여야 한다.

「의료법」시행규칙 별지 제9호의2 서식 <개정 2015. 5. 29>

진료기록 열람 및 사본발급 동의서

환자 본인	성명	연락처
	생년월일(외국인등록번호)	
	주소	
신청인	성명	환자와의 관계
	생년월일(외국인등록번호)	연락처
	주소	

「의료법」시행규칙 별지 제9호의2 서식 <개정 2014. 8. 6>

진료기록 열람 및 사본발급 위임장

수임인	성명	전화번호
	생년월일(외국인등록번호)	위임인과의 관계
	주소	
위임인	성명	전화번호
	생년월일(외국인등록번호)	
	주소	

위임인은 「의료법」 제21조제2항 및 같은 법 시행규칙 제3조의에 따라 「진료기록 등 열람 및 사본발급 동의서」에 기재된 사항에 대하여 일체 권한을 상기 수임인에게 위임합니다.

참고자료

- 보건복지부 · 행정자치부, 「개인정보보호 가이드라인 [의료기관 편]」, 2015. 2.

38 헌혈자의 주민등록번호 수집 · 이용

Q 헌혈과 혈액관리를 위해서 주민등록번호를 수집 · 이용할 수 있는지요?

A 헌혈자의 신원확인, 채혈금지대상자의 관리 등을 위해서 헌혈자의 신분을 명확히 확인할 필요성이 있으며 관련 법령에 헌혈 · 혈액관리를 위한 주민등록번호 처리 허용근거도 마련되어 있으므로, 주민등록번호의 수집 · 이용이 허용됩니다.

상세 설명

「혈액관리법」은 개인이 자기의 혈액을 혈액원에 무상으로 제공하는 헌혈 및 혈액관리 사무에 대한 제반 처리근거를 상세히 마련하여 두고 있습니다.

* '혈액원'이란 혈액관리업무를 수행하기 위하여 보건복지부장관의 허가를 받은 자를 말하며, 여기에는 의료기관 및 대한적십자사 등이 있음 (「혈액관리법」제2조제3호)

헌혈 및 혈액관리업무에 있어서는 부적격혈액의 수혈 등 혈액사고 발생을 방지하기 위한 제반 조치와 더불어 헌혈자의 명확한 식별이 필요합니다. 이에 따라 「혈액관리법」은 헌혈자에 대해 신원확인과 건강검진을 실시하고 신원이 확실하지 않거나 신원 확인에 필요한 요구에 따르지 아니하는 사람으로부터는 채혈을 하지 않도록 하고(「혈액관리법」제7조), 보건복지부장관은 채혈금지대상자의 명부를 작성 · 관리할 수 있도록 하면서 채혈금지대상자로부터 채혈을 하지 않도록 규정하고 있습니다(「혈액관리법」제7조의2). 그리고 이들 업무를 위하여 보건복지부장관 및 혈액원이 주민등록번호 등의 고유식별정보 및 민감정보를 처리할 수 있는 근거 규정을 마련하여 두고 있습니다(「혈액관리법」시행령 제10조의2). 따라서 대한적십자사 등 혈액원은 헌혈과 혈액관리 업무를 위하여 상기 법령이 규정한 업무범위 내에서 주민등록번호를 수집 · 이용할 수 있습니다.

그런데, 헌혈자에 대한 건강진단을 하는 경우에는 원칙적으로 사진이 붙어 있어 본인임을 확인할 수 있는 주민등록증, 여권 등의 신분증명서에 따라 그 신원을 확인하여야 하지만, 학생·군인 등의 단체 헌혈의 경우에는 그 관리·감독자의 확인으로 갈음할 수 있습니다(「혈액관리법」시행규칙 제6조제1항). 따라서 학교 등의 단체헌혈의 경우에는 학교 보건교사 등이 신원확인을 하는 것으로 대신하고, 반드시 전교생의 명렬표와 주민등록번호를 혈액원에 제공해야 할 필요성은 없습니다(교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12 참조).

관련 법령

「혈액관리법」시행령

제10조의2(민감정보 및 고유식별정보의 처리) 보건복지부장관(제10조에 따라 보건복지부장관의 권한 등을 위임·위탁받은 자를 포함한다) 또는 혈액원은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강, 성생활에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제6조에 따른 혈액관리업무 및 혈액원 개설 등에 관한 사무
2. 법 제7조에 따른 헌혈자의 신원확인 및 건강진단 등에 관한 사무
3. 법 제7조의2에 따른 채혈금지대상자의 관리에 관한 사무
4. 법 제8조에 따른 혈액의 안전성 확보에 관한 사무
5. 법 제8조의2에 따른 혈액사고발생시 조치 등에 관한 사무
6. 법 제10조에 따른 특정수혈부작용에 대한 조치에 관한 사무
7. 법 제10조의2에 따른 특정수혈부작용 및 채혈부작용의 보상에 관한 사무
8. 법 제12조에 따른 혈액관리업무에 관한 기록의 작성 등에 관한 사무
9. 법 제12조의2에 따른 전자혈액관리업무기록의 작성 등에 관한 사무
10. 법 제13조에 따른 품질관리 검사 등에 관한 사무
11. 법 제14조에 따른 헌혈증서의 교부 및 환부 등에 관한 사무
12. 법 제17조의2에 따른 혈액원의 개설허가 취소 등에 관한 사무

「혈액관리법」시행규칙

제6조(헌혈자의 건강진단 등) ① 법 제7조제1항에 따라 혈액원은 헌혈자로부터 채혈하기 전에 사진이 붙어 있어 본인임을 확인할 수 있는 주민등록증, 여권, 학생증, 그 밖의 신분증명서에 따라 그 신원을 확인하여야 한다. 다만, 학생, 군인 등의 단체헌혈의 경우 그 관리·감독자의 확인으로 갈음할 수 있다. (이하 생략)

「혈액관리법」시행규칙 별지 제1호의8 서식 (채혈금지대상자 관리대장)

[별지 제1호의8서식] <신설 2009.1.30>

채혈금지대상자 관리대장

일련번호	주민등록번호	성명	채혈금지사유	채혈금지기간

제 6 장

금융·보험·상거래 사례

제6장 금융 · 보험 · 상거래 사례

39 CMS(자금이체서비스) 이용을 위한 주민등록번호 처리

Q **CMS(자금이체서비스)를 이용하기 위하여 출 · 입금 신청 등을 하는 경우에 주민등록번호를 기재하는 것이 허용되는지요?**

A CMS 이용기관 등은 고객으로부터 출금이체신청서 접수 등의 경우에 주민등록번호 대신 생년월일(주민등록 상) 정보를 수집 · 이용하여야 합니다.

상세 설명

CMS(Cash Management Service; 자금이체서비스)는 은행 등의 금융기관 및 이용기관의 전산시스템을 상호 접속시켜 이용기관이 은행 및 증권사 등의 고객계좌에서 자금을 출금이체 또는 고객계좌로 입금이체할 수 있는 서비스를 말합니다. CMS 서비스는 자금이체 과정이 안정적이고 신뢰할 수 있으며 편의에 따라 각종 대금의 납부방법이나 납기일을 선택할 수 있고 각종 자금의 수납이 손쉬워서 사회 전반에 걸쳐 널리 이용되고 있습니다(금융결제원 홈페이지 www.cmsedi.or.kr → CMS 이용안내 참조).

CMS를 이용하려 하는 경우, 과거에는 출금이체신청서 등에 납부자의 성명, 금융기관명, 예금계좌번호 등과 함께 주민등록번호(사업자의 경우 사업자등록번호)를 기재하도록 하였습니다. 그러나 「개인정보 보호법」개정으로 '14. 8. 7일부터 주민등록번호 처리 법정주의가 시행됨에 따라 주민등록번호를 처리하기 위해서는 반드시 법령에 구체적인 처리 요구 · 허용 근거가 필요하게 되었습니다. 그런데 CMS의 경우 반드시 주민등록번호를 기재하도록 해야 할 불가피성이 있지 않았으며, CMS를 위한 주민등록번호 처리 법령근거도 존재하지 않았습니다.

이에 따라, CMS를 제공하는 기관 등은 출금이체신청서 등에 주민등록번호를 기재하도록 하여서는 아니되며, 고객의 생년월일을 기재하여야 합니다. 또한 CMS를 제공하는 기관은 CMS에 사용되는 전산시스템에서 주민등록번호 필드를 생년월일 필드로 변경하는 등의 조치를 이행하여야 합니다.

참고자료

- 금융위원회 · 금융감독원, 「금융분야 주민등록번호 수집 · 이용 가이드라인」, 2015. 1.
- 금융결제원, "개인정보보호법 개정에 따른 CMS 이용기관 조치사항", 2014. 5.

40 수표 거래 시 주민등록번호 배서

Q 수표 거래 시에 주민등록번호를 배서하여도 되는지요?

A 개인 간의 수표 거래 시에 주민등록번호를 배서하는 것은 금지됩니다. 다만 상대방의 신분확인을 위하여 주민등록번호가 기재된 신분증 제시를 요구 · 열람하는 것은 가능합니다.

상세 설명

거래를 위하여 수표를 유통하는 경우에는 '배서'(背書)에 의해 양도할 수 있습니다(「수표법」제14조제1항). 배서는 수표 또는 이에 결합한 보충지에 적고 배서인이 기명날인하거나 서명하는 방식으로 이루어집니다(「수표법」제16조제1항).

과거에는 수표 뒷면의 배서란에 성명, 주민등록번호, 주소, 연락처 등의 사항을 기재하는 경우가 종종 있었으나, 현재의 수표 양식에는 주로 성명, 실명확인번호, 연락처 등을 배서하도록 하고 있습니다. 다만 '실명확인번호'가 정확히 무엇을 말하는지에 대한 법령 규정 등이 존재하지 않은 관계로 수표 배서 시에 어떠한 기재사항을 적어야 하는지에 대한 논란이 있어 왔으며, 관행적으로 주민등록번호 배서를 요구하는 경우도 종종 발생하여 왔습니다.

그러나 「개인정보 보호법」개정으로 '14. 8. 7일부터 주민등록번호 처리 법정주의가 시행됨에 따라 주민등록번호를 처리하기 위해서는 반드시 법령에 구체적인 처리 요구 · 허용 근거가 있어야 합니다. 하지만 「수표법」에서는 배서 시에 기명날인 또는 서명하도록 규정하고 있을 뿐 주민등록번호 배서에 대해서는 명시적인 규정이 존재하지 않습니다. 따라서, 개인 간의 수표 유통 · 양도 시에 주민등록번호를 배서하거나 배서를 요구하는 것은 허용되지 않습니다.

다만 상대방의 신원확인 등을 위하여 신분증을 확인하는 것은 가능합니다. 한편 「금융실명거래 및 비밀보장 등에 관한 법률」에 따라 금융회사가 수표의 발생 · 수납 등의 업무를 하는 경우에는 거래자의 주민등록번호를 수집 · 보관할 수 있습니다(금융위원회 · 금융감독원, 「금융분야 주민등록번호 수집 · 이용 가이드라인」, 2015. 1 참조).

관련 법령

「수표법」

제14조(당연한 지시증권성) ① 기명식 또는 지시식의 수표는 배서에 의하여 양도할 수 있다.

제16조(배서의 방식) ① 배서는 수표 또는 이에 결합한 보충지[보전]에 적고 배서인이 기명날인하거나 서명하여야 한다.

참고자료

• 금융위원회 · 금융감독원, 「금융분야 주민등록번호 수집 · 이용 가이드라인」, 2015. 1.

41 긴급한 금융업무 처리시 주민등록번호 이용

Q **고객이 통장이나 카드를 분실하여 은행에 비밀번호 변경이나 지급정지 등 긴급 요청시, 고객정보 조회를 위해 주민등록번호를 이용할 수 있습니까?**

A 고객의 급박한 재산상 이익을 위하여 명백히 필요하다고 인정되는 경우, 주민등록번호 외에 다른 정보를 통해 업무를 처리하는 것이 명백히 곤란하다면 주민등록번호를 처리할 수 있습니다.

상세 설명

계좌번호나 카드번호를 기억하지 못하는 고객이 불의의 사고 등으로 통장이나 카드 등을 분실하여 해당 금융기관에 비밀번호 변경이나 지급 정지 등의 긴급조치를 요구하는 경우, 금융기관이 해당 고객에게 주민등록번호를 알려달라고 한 후 계좌 또는 카드 정보를 조회하여 긴급조치를 해야만 하는 경우가 있을 수 있습니다.

개인정보처리자는 다음의 사유에 해당하는 경우에는 예외적으로 주민등록번호를 처리할 수 있습니다 (「개인정보 보호법」 제24조의2제1항).

1) 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2) 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3) 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

그러므로 개인정보보호법 제24조의2제1항제2호에 따라 개인정보처리자는 정보주체 또는 제3자의 급박한 생명 · 신체 · 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 주민등록번호를 처리할 수 있습니다.

위 질의 내용과 같이 통장 또는 카드 분실로 인한 정보주체의 급박한 재산상 피해를 예방하기 위하여 금융기관의 긴급한 조치가 필요한 경우로서 계좌번호나 카드번호 분실 또는 미인지로 인하여 주민등록번호 외 다른 정보를 통해 업무를 처리하는 것이 명백히 곤란한 경우라면 개인정보보호법 제24조의2제1항제2호가 적용될 수 있는 경우에 해당될 수 있을 것입니다.

관련 법령

「개인정보 보호법」

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

42 단체보험 가입을 위한 주민등록번호 처리

Q **임직원에 대한 상해보험, 여행자보험 등의 단체보험 가입 처리를 위하여 주민등록번호를 수집 · 이용할 수 있습니까?**

A 기업 등은 단체보험 가입계약 체결을 위하여 보험업법 시행령에 따라 피보험자인 임직원의 주민등록번호를 수집하여 보험회사에 제공할 수 있습니다.

상세 설명

기업이나 공공기관 등에서는 소속 임직원의 안전 및 복리후생 등을 위하여 생명보험, 상해 · 질병보험 등을 단체로 가입 처리하는 경우가 다수 있습니다. 또한 각종 기관 · 단체 등에서는 외부인을 대상으로 하는 각종 스포츠 · 문화 행사 개최 시에도 참석자를 대상으로 단체보험 가입을 하는 경우가 있으며, 여행자보험을 단체로 가입하도록 하는 경우 또한 존재합니다.

이와 같이 보험회사가 타인을 위한 보험계약(「상법」제639조)이나 단체보험계약(「상법」제735조의3)을 체결하는 경우에는 주민등록번호를 포함한 고유식별정보나 건강정보의 수집 · 이용이 필요할 수 있습니다. 이에 따라 「보험업법」시행령 제102조제5항에서는 보험회사는 타인을 위한 보험계약 또는 단체보험계약의 체결, 유지 · 관리, 보험금의 지급 등에 관한 사무를 위하여 피보험자의 건강정보 또는 주민등록번호를 포함한 고유식별정보를 처리할 수 있도록 명확한 근거 규정을 두고 있습니다. 따라서 보험회사는 타인을 위한 보험계약 또는 단체보험계약 체결 등을 위해 주민등록번호를 처리할 수 있습니다.

한편 타인을 위한 보험계약이나 단체보험계약의 당사자인 기업이나 공공기관, 각종 기관 · 단체 등도 당연히 피보험자의 주민등록번호를 수집하여 보험회사에 전달하여야 하므로 이 역시 주민등록번호 처리의 불가피성이 인정된다 하겠습니다. 또한 임직원의 가족 등에 대해서 단체보험 가입을 처리하는 경우에도 마찬가지입니다. 다만 보험계약을 위해 새로 수집한 주민등록번호는 보험계약 체결을 위해 보험회사에 전달 후 별도의 보관 필요성이 없는 경우에는 즉시 파기하는 조치가 필요합니다.

관련 법령

「보험업법」시행령

제102조(민감정보 및 고유식별정보의 처리) ⑤ 보험회사는 다음 각 호의 사무를 수행하기 위하여 필요한 범위로 한정하여 해당 각 호의 구분에 따라 「개인정보 보호법」 제23조에 따른 민감정보 중 건강에 관한 정보(이하 이 항에서 "건강정보"라 한다)나 같은 법 시행령 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호(이하 이 항에서 "고유식별정보"라 한다)가 포함된 자료를 처리할 수 있다.

1. 「상법」 제639조에 따른 타인을 위한 보험계약의 체결, 유지·관리, 보험금의 지급 등에 관한 사무: 피보험자에 관한 건강정보 또는 고유식별정보
4. 「상법」 제735조의3에 따른 단체보험계약의 체결, 유지·관리, 보험금지급 등에 관한 사무: 피보험자에 관한 건강정보 또는 고유식별정보

「상법」

제639조(타인을 위한 보험) ①보험계약자는 위임을 받거나 위임을 받지 아니하고 특정 또는 불특정의 타인을 위하여 보험계약을 체결할 수 있다. 그러나 손해보험계약의 경우에 그 타인의 위임이 없는 때에는 보험계약자는 이를 보험자에게 고지하여야 하고, 그 고지가 없는 때에는 타인이 그 보험계약이 체결된 사실을 알지 못하였다는 사유로 보험자에게 대항하지 못한다.

②제1항의 경우에는 그 타인은 당연히 그 계약의 이익을 받는다. 그러나 손해보험계약의 경우에 보험계약자가 그 타인에게 보험사고의 발생으로 생긴 손해의 배상을 한 때에는 보험계약자는 그 타인의 권리를 해하지 아니하는 범위안에서 보험자에게 보험금액의 지급을 청구할 수 있다.

③제1항의 경우에는 보험계약자는 보험자에 대하여 보험료를 지급할 의무가 있다. 그러나 보험계약자가 파산선고를 받거나 보험료의 지급을 지체한 때에는 그 타인이 그 권리를 포기하지 아니하는 한 그 타인도 보험료를 지급할 의무가 있다. 제735조의3(단체보험)

①단체가 규약에 따라 구성원의 전부 또는 일부를 피보험자로 하는 생명보험계약을 체결하는 경우에는 제731조를 적용하지 아니한다.

②제1항의 보험계약이 체결된 때에는 보험자는 보험계약자에 대하여서만 보험증권을 교부한다.

③ 제1항의 보험계약에서 보험계약자가 피보험자 또는 그 상속인이 아닌 자를 보험수익자로 지정할 때에는 단체의 규약에서 명시적으로 정하는 경우 외에는 그 피보험자의 서면동의를 받아야 한다.

참고자료

• 행정자치부, 주민등록번호 수집 금지 제도 가이드라인, 2014. 1.

43 귀금속 거래 시 주민등록번호 수집

Q **귀금속 상점에 금반지를 팔려고 했더니, 주민등록번호를 적어달라고 하고 신분증도 복사해야 한다고 합니다. 그렇게 하지 않으면 금 거래를 할 수 없다고 하는데, 정말 그런 것인지요?**

A 귀금속 상점에서 금붙이 등을 매입하려 할 때에는 고객의 주민등록번호를 수집하지 말고 필요시 신분증 확인을 통하여 이름 및 생년월일 등 최소한의 개인정보만 처리하도록 해야 합니다.

상세 설명

귀금속 상점에서는 물건을 팔 때와 달리, 고객으로부터 귀금속을 매입하려는 경우 대상 물건이 장물일 경우 사후 조치 등을 위하여 주민등록증을 복사하여 두거나 주민등록번호를 수집하는 것이 관행적이었습니다.

그러나 주민등록번호는 관련 법령에 구체적으로 허용하거나 요구하는 근거가 있어야만 처리가 가능하기 때문에, 귀금속 거래시에 상대방의 신분을 확인할 필요가 있다 하더라도 그러한 이유만으로는 주민등록번호를 수집할 근거가 있다고 할 수 없습니다.

따라서 귀금속 매입시에도 매도자의 주민등록번호가 기재된 신분증은 육안으로만 확인을 하고, 필요 최소한의 고객정보인 이름과 생년월일 등만 수집하도록 해야 할 것입니다.

한편 「개인정보 보호법」제16조는 개인정보처리자가 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다고 규정하고 있습니다. 또한 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 됩니다.

그러므로 해당 거래에 필요 최소한의 정보를 수집할 수 있는데도 불구하고, 고객이 주민등록번호 수집을 거절한다는 이유만으로 귀금속 거래를 거절해서는 안 되며, 업계에서 관행적으로 수집하여 보관하고 있던 기존의 주민등록번호도 2016. 8. 6. 전에 삭제하도록 개선되어야 합니다.

44 해외구매대행 서비스 이용 시 주민등록번호 처리

Q **해외 구매대행 서비스를 이용하는 과정에서 주민등록번호 입력이 반드시 필요한지요? 최근 주민등록번호 대신 '개인통관고유부호'를 발급받으라고 하는데 이는 무엇인가요?**

A 개인물품을 해외에서 구매하여 수입신고하는 경우에는 주민등록번호 또는 관세청에서 부여하는 '개인통관고유부호'를 사용할 수 있습니다. 다만 해외 구매대행 또는 배송대행 서비스 업체는 관련 법령에 주민등록번호 처리 허용 근거가 없으므로 개인통관고유부호를 사용해야 합니다.

상세 설명

개인이 해외로부터 물품을 구매(수입)하는 경우에는 「관세법」등이 정하는 바에 따라 수입신고를 하여야 하고(「관세법」제241조), 이때의 신고사항은 납세의무자 또는 화주의 상호(개인인 경우 성명), 사업자등록번호, 통관고유부호 등입니다(「관세법」시행령 제246조). 그리고 관세청장, 세관장, 세관공무원은 관세의 부과 · 징수, 수출입물품의 통관에 관한 사무를 처리하기 위해 불가피한 경우 주민등록번호 등 고유식별정보가 포함된 자료를 처리할 수 있도록 법적 근거가 마련되어 있습니다(「관세법」시행령 제289조).

특히 관세청은 수출입신고 절차에서 개인정보 유출을 방지하기 위하여 주민등록번호 대신 활용할 수 있는 '개인통관고유부호 제도'를 운영하고 있습니다. 따라서 개인이 해외에서 물품을 구매하고 수입신고를 하는 경우에는 주민등록번호 또는 개인통관고유부호 중에서 선택적으로 사용할 수 있지만, 주민등록번호는 정보 유출 위험성 및 2차 악용 가능성이 높으므로 가급적 개인통관고유부호를 발급받아 이용하는 것이 좋습니다.

* 개인통관고유부호 번호체계 : 개인부호(P) + 출생년도(2) + 성별(1) + 발급년도(2) + 고유번호(6) + 오류검증부호(1) 의 총 13자리로 이루어져 있음

* 개인통관고유부호는 관세청 전자통관시스템(portal.customs.go.kr)에서 신청 즉시 부여되며 한번 부여받은 번호는 같은 번호로 계속 반복하여 사용 가능 (발급신청시 원칙적으로 공인인증서 필요)

한편 최근에는 이른바 해외직구가 많이 이용되면서 해외 구매대행나 배송대행 업체를 이용하는 경우가 많이 있습니다. 주민등록번호 처리금지 원칙이 시행('14.8.7)되기 이전에는 이들 업체가 관세 신고 및 확인 등을 이유로 고객에게 주민등록번호를 요구하는 경우가 많았습니다.

그러나 현재는 이들 구매대행이나 배송대행 업체들이 주민등록번호를 수집·이용할 명시적 법적 근거가 「관세법」 등에 없습니다. 따라서 이들 업체는 고객의 주민등록번호를 요구하거나 수집할 수 없으며 개인통관부호를 이용하여 서비스를 제공해야 할 것입니다.

관련 법령

「관세법」시행령

제289조(민감정보 및 고유식별정보의 처리) ① 관세청장, 세관장 또는 세관공무원은 법 및 이 영에 따른 관세의 부과·징수 및 수출입물품의 통관에 관한 사무를 처리하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 정보나 같은 영 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

「통관고유부호 및 해외거래처부호 등록 · 관리에 관한 고시」

제1조(목적) 이 고시는 「관세법」 제241조 및 같은 법 시행령 제246조에 따른 통관고유부호 및 해외거래처부호의 등록과 관리에 필요한 사항을 정함으로써 수출입통관업체 또는 개인별 식별부호를 정확하게 부여하고 관리하여 수출입통관업무의 적정을 기함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음과 같다.

1. "통관고유부호"란 수출입통관업체 또는 개인의 식별을 위하여 통관고유부호 체계(별표 1, 2)에 따라 부호관리시스템에서 부여한 부호를 말한다. (이하 생략)

참고자료

• 관세청, '「개인통관고유부호」 관련 자주하는 질문-답변 사례 모음', 2014. 8.

45 렌터카 서비스 계약 시 주민등록번호 수집 · 이용

Q **여행지에서 렌터카를 이용하려고 했더니 주민등록번호를 기재해야 한다고 하는데, 어차피 운전면허증을 제시하고 빌리는 것인데 꼭 주민등록번호까지 적어야 하는지요?**

A 렌터카 회사에서 고객의 주민등록번호를 수집하도록 허용하는 근거 법령은 없기 때문에, 운전면허번호로 대체하여야 하며 신분증 사본의 수집시에도 이 점을 유의해야 합니다.

상세 설명

렌터카 거래는 고가의 물품을 대상으로 하는 것이어서 그 동안 해당 업계에서는 대부분 고객의 주민등록번호를 수집하여, 차량파손이나 교통법규 위반 범칙금 처리에 대비하는 것이 관행이었습니다.

그러나 아무리 고가의 물품에 대한 거래라 하더라도, 일반적인 상거래 관계에서 고객의 주민등록번호를 수집할 수 있도록 허용하는 구체적 근거 법령은 없습니다.

그러므로 차량의 파손이나 범칙금 처리와 같이 향후 발생할 지도 모르는 분쟁에 대비하기 위하여 이들 업체에서 고객의 주민등록번호를 수집하는 관행은 더 이상 허용되지 아니하며, 렌터카 대여계약서 작성시 운전자의 운전면허번호를 별도의 동의를 받아 수집하여 보관하도록 개선되어야 합니다.

* 운전면허번호는 「개인정보 보호법」 제24조에서 규정하는 고유식별정보에 해당되기 때문에, 운전면허번호를 수집하여 처리하는 경우에도 관련 법령에서 구체적으로 허용하거나 요구하는 근거가 없는 한, 정보주체로부터 별도의 동의를 받아야만 처리가 허용됨

한편 운전면허증에는 면허번호와 함께 주민등록번호도 기재가 되어 있으므로, 면허증 사본을 수집하려는 경우에는 주민등록번호가 함께 수집되지 않도록 조치하여 보관해야 합니다.

나아가 렌터카 이용자가 세금계산서 발행을 요청하는 경우, 「부가가치세법」 제32조 제1항에 따라 사업자가 재화 또는 용역을 공급(부가가치세가 면제되는 재화 또는 용역의 공급은 제외)하는 경우에는 그 공급을 받는 자에게 세금계산서를 발급하여야 하며, 동 세금계산서에는 사업자 등록번호나 고유번호 또는 주민등록번호를 기재토록 하고 있는 바, 세금계산서를 발급받는 자가 사업자 등록번호나 고유번호가 없는 경우에는 주민등록번호를 기재한 세금계산서 발행이 가능합니다. 다만, 이 경우에도 세금계산서 발급과 국세청 신고를 목적으로 수집한 주민등록번호는 당초 수집 목적과 다른 용도로 이용하거나 제3자에게 제공할 수 없으며 특히, 「부가가치세법」 제71조 제3항에 따라 전자세금계산서의 형태로 세금계산서를 발급한 경우에는 국세청에 전자세금계산서 발급명세를 전송한 이후 별도로 주민등록번호를 저장 · 보관할 수 없습니다.

관련 법령

「개인정보 보호법」

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

「개인정보 보호법」 시행령

제19조(고유식별정보의 범위)법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보(이하 "고유식별정보"라 한다)를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다

1. 「주민등록법」 제7조제3항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제4항에 따른 외국인등록번호

제 7 장

교육기관 사례

제 7 장 교육기관 사례

46 교육정보시스템(NEIS) 입력 위한 학부모 · 보호자의 주민등록번호 수집 · 이용

Q **초 · 중 · 고교에서 교육정보시스템(NEIS)에 학부모나 보호자 확인과 정보 입력을 위하여 주민등록번호를 수집하거나 주민등록등본 · 가족관계등록부 등을 수합하여도 되는지요?**

A 학교생활기록 및 교육정보시스템(NEIS)에는 학부모의 주민등록번호를 수집하여 입력해서는 아니 됩니다. 다만 주소와 보호자 확인 등을 위해 주민등록등본 등을 요청 · 수합하는 경우에는 주민등록등본 뒷자리가 마스킹 처리된 주민등록등본을 요청하는 등의 방법을 이용할 수 있습니다.

상세 설명

초 · 중 · 고등학교는 학생의 학업성취도와 인성 등을 종합적으로 관찰 · 평가하여 학생지도 및 상급학교의 학생 선발에 활용할 수 있도록 '학교생활기록'을 작성하여 관리하도록 의무화하고 있습니다. 학교생활기록에는 1) 인적사항, 2) 학적사항, 3) 출결상황, 4) 자격증 및 인증취득상황, 5) 교과학습 발달상황, 6) 행동특성 및 종합의견 등의 자료를 작성하여야 하고, 이들 자료는 교육정보시스템(NEIS)로 작성 · 관리하도록 하고 있습니다(「초 · 중등교육법」제25조). 특히 인적사항에는 학생의 성명 · 주민등록번호 · 주소(입학당시 주소를 입력하고, 재학 중 주소 변경시에는 변경된 주소를 누가 입력), 학부모의 성명 · 생년월일 및 가족의 변동 특기사항(학생 이해에 도움이 될 수 있는 내용이 있는 경우 본인 또는 보호자의 동의를 받아 입력) 등을 작성하도록 규정하고 있습니다.

주민등록번호를 처리하기 위해서는 반드시 관련 법령에서 주민등록번호의 처리를 요구 · 허용하는 근거 규정이 필요합니다. 따라서 교육정보시스템(NEIS)를 통하여 학교생활기록을 작성하는 경우에는 학생의 주민등록번호는 입력 필요가 있으나, 학부모의 주민등록번호는 입력하여서는 안되며 생년월일 정보를 기재해야 합니다.

다만 예외적으로, 학생 · 학부모의 실재 주소 확인이나 보호자 여부 확인을 위해서 주민등록등본이나 가족관계등록부 등의 공부(公簿)가 필요할 수도 있습니다. 이러한 경우에는 주민등록번호 뒷자리가 마스킹(***) 처리된 서류를 요청하거나, 주민등록번호 뒷자리까지 표시되

어 있는 경우에는 뒷자리를 삭제 처리하거나, 또는 서류를 확인만 하고 돌려주는 방법 등을 이용할 수 있습니다(교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12 참조).

* 주민등록번호 앞자리만을 수집·이용하거나, 주민등록번호가 기재된 신분증이나 공부(公簿) 서류를 단순히 확인만 하고 반환하는 행위 등은 '주민등록번호 처리'에 해당하지 않는 것으로 간주

관련 법령

「초 · 중등 교육법」

제25조(학교생활기록) ① 학교의 장은 학생의 학업성취도와 인성( ) 등을 종합적으로 관찰·평가하여 학생지도 및 상급학교(「고등교육법」 제2조 각 호에 따른 학교를 포함한다. 이하 같다)의 학생 선발에 활용할 수 있는 다음 각 호의 자료를 교육부령으로 정하는 기준에 따라 작성·관리하여야 한다.

1. 인적사항
2. 학적사항
3. 출결상황
4. 자격증 및 인증 취득상황
5. 교과학습 발달상황
6. 행동특성 및 종합의견
7. 그 밖에 교육목적에 필요한 범위에서 교육부령으로 정하는 사항

② 학교의 장은 제1항에 따른 자료를 제30조의4에 따른 교육정보시스템으로 작성·관리하여야 한다.

「초 · 중등 교육법」시행규칙

제21조(학교생활기록의 작성기준) ① 법 제25조제1항에 따라 법 제2조에 따른 학교(이하 "학교"라 한다)의 장은 다음 각 호의 작성기준에 따라 학교생활기록을 작성하여야 한다.

1. 인적사항: 학생의 성명·주민등록번호 · 주소와 부모의 성명·생년월일 및 가족의 변동사항 등 (이하 생략)

참고자료

• 교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12.

47 대학 입학전형 위한 지원자 주민등록번호 수집 · 이용

Q **대학교 등에서 일반전형이나 특별전형 등 학생 선발을 위하여 주민등록번호를 수집 · 이용할 수 있는지요?**

A 대학 등 「고등교육법」의 적용을 받는 학교는 학생의 선발을 위하여 지원 원서에 주민등록번호를 기재하도록 하거나 학교생활기록부를 받는 등 주민등록번호를 수집 · 이용할 수 있습니다.

상세 설명

고등교육을 실시하기 위한 학교에는 대학, 산업대학, 교육대학, 전문대학, 원격대학(방송대학, 통신대학, 방송통신대학, 사이버대학), 기술대학 등이 있습니다(「고등교육법」제2조). 이러한 고등교육을 실시하는 학교(이하 '대학'이라 칭함)에 입학할 수 있는 사람은 고등학교를 졸업한 사람이나 법령에 따라 이와 같은 수준 이상의 학력이 있다고 인정된 사람이어야 하며(「고등교육법」제33조제1항), 대학은 위의 학력 자격이 있는 사람 중에서 일반전형이나 특별전형에 의하여 입학을 허가할 학생을 선발할 수 있습니다.

대학의 장은 입학전형을 위하여 고등학교 학교생활기록부, 대학수학능력시험의 성적, 대학별 고사(논술 등 필답고사, 면접 · 구술고사, 신체검사, 실기 · 실험고사, 교직적성 · 인성검사) 성적, 자기소개서 등 교과성적 외의 자료를 입학전형자료로 활용할 수 있으며(「고등교육법」시행령 제35조), 실제로 각 대학등은 입학전형을 위하여 학교생활기록부 사본, 검정고시 합격증명서 사본, 졸업증명서 사본 등을 지원자에게 요구하고 있습니다.

이를 위하여 「고등교육법」시행령은 교육부장관, 대학의 장, 학교협의체(한국대학교육협의회, 한국전문대학교육협의회 등)는 학생 선발에 관한 사무, 대학수학능력시험에 관한 사무, 입학지원방법 위반자의 처리에 관한 사무를 위하여 주민등록번호가 포함된 자료를 처리할 수 있도록 하고 있습니다(「고등교육법」시행령 제73조제1항). 또한 고등학교 학교생활기록부에는 관련 법령에 따라 학생의 성명, 주민등록번호, 주소 등을 포함한 학생 인적사항을 기재하여야 하고(「초중등교육법」시행규칙 제21조), 고등학교졸업학력검정고시 합격증명서에도 해당자의 성명, 주민등록번호를 기재하도록 하고 있으므로(「초중등교육법」시행규칙 별지 제11호 서식) 대학 입학전형을 위하여 이러한 자료를 활용하도록 한 규정 역시도 주민등록번호의 처리 근거로 볼 수 있습니다. 따라서 결론적으로, 대학은 학생 선발을 위하여 지원자의 주민등록번호를 수집 · 이용할 수 있습니다.

한편, 대다수의 대학은 학생 선발 전형에 있어 온라인 원서접수 방식을 채택하고 있으며, 이를 위하여 민간 온라인 원서접수 전문기관에 관련 사무를 위탁하는 것이 일반적입니다. 만약 대학과 온라인 원서접수 전문기관(수탁자) 간에 개인정보 처리위탁을 위한 제반 절차가 적법하게 준수되었다면(「개인정보 보호법」제26조 참조), 온라인 원서접수 전문기관도 해당 대학의

학생 선발 전형업무 수탁에 따라 주민등록번호 수집 · 이용이 허용됩니다.

* 개인정보처리자는 제3자에게 개인정보 처리업무를 위탁할 수 있으며, 이 경우

1) 위탁업무 수행 목적 외 개인정보 처리금지에 관한 사항, 개인정보의 기술적·관리적 보호조치에 관한 사항, 기타 개인정보의 안전한 관리를 위하여 필요한 사항이 포함된 문서로 위탁 처리

2) 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개

3) 업무위탁으로 인해 정보주체 개인정보가 분실, 도난, 유출, 변조, 훼손되지 아니하도록 수탁자를 교육하고 개인정보를 안전하게 처리하는 지를 감독하는 등 제반 조치를 이행하여야 함

(「개인정보 보호법」 제26조 참조)

관련 법령

「고등교육법」시행령

제73조(고유식별정보의 처리) ① 교육부장관, 대학의 장 및 학교협의체는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제34조제1항에 따른 학생 선발에 관한 사무
2. 법 제34조제3항에 따른 시험에 관한 사무
3. 제42조의2에 따른 입학지원방법 위반자의 처리에 관한 사무

「초 · 중등교육법」 시행규칙

제21조(학교생활기록의 작성기준) ① 법 제25조제1항에 따라 법 제2조에 따른 학교(이하 "학교"라 한다)의 장은 다음 각 호의 작성기준에 따라 학교생활기록을 작성하여야 한다.

1. 인적사항: 학생의 성명·주민등록번호·주소와 부모의 성명 · 생년월일 및 가족의 변동사항 등 (이하 생략)

48 스쿨뱅킹 서비스를 위한 주민등록번호 수집 · 이용

Q **학생들로부터 스쿨뱅킹 서비스 신청서를 접수받을 때 학부모(예금주) 등의 주민등록번호를 수집 · 이용할 수 있는지요?**

A 스쿨뱅킹 서비스에는 주민등록번호 수집 · 이용에 대한 법령 근거가 없으므로 주민등록번호 수집 · 이용이 금지됩니다.

상세 설명

'스쿨뱅킹'이란 초 · 중 · 고교 등 각급 학교의 각종 납부금, 즉 급식비, 현장학습비, 특기정석교육 활동비, 등록금 등을 학부모가 일일이 개별적으로 납부할 필요 없이, 학부모 계좌에서 학교 수납 계좌로 자동 이체하는 서비스를 말합니다. 일반적으로 스쿨뱅킹은 학교가 지정한 금융회사와 연계하여 이루어지고, 학부모들은 스쿨뱅킹 자동납부 신청서를 작성하여 이용하게 됩니다. 스쿨뱅킹은 현장에서 현금으로 각종 납부금을 내는 경우의 도난 · 분실 문제를 해소할 수 있고 학부모의 번거로움을 줄여주며 학교 측의 수납업무로 인한 부담도 줄여준다는 측면에서 다수의 학교에서 널리 이용되고 있습니다.

다만 스쿨뱅킹 서비스를 위한 개인정보 처리에 관한 명확한 법적 근거가 마련되어 있지는 않으며, 학교의 필수적인 소관 업무의 범위에 해당한다고 보기도 어렵습니다. 특히 주민등록번호 처리가 허용되기 위해서는 관련 법령에 주민등록번호 처리를 요구 · 허용하는 명확한 근거가 마련되어 있어야 하는데, 스쿨뱅킹 서비스와 같은 CMS(Cash Management Service; 자금이체서비스)는 반드시 주민등록번호를 기재해야 할 불가피성이 있지 않으며 CMS를 위한 주민등록번호 처리 법령근거도 존재하지 않습니다. 따라서 스쿨뱅킹 서비스 신청서 등에는 주민등록번호를 기재하도록 하여서는 안되며, 생년월일 등으로 대체하여야 합니다.

참고자료

- 교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12.
- 금융결제원, "개인정보보호법 개정에 따른 CMS 이용기관 조치사항", 2014. 5.

49 장학금 신청 · 심사 및 지급을 위한 주민등록번호 수집 · 이용

Q **국가 · 지방자치단체, 장학재단, 대학 등에서 장학금을 지급하기 위하여 대상자의 주민등록번호를 수집 · 이용할 수 있는지요?**

A 국가장학금의 신청 · 심사를 위해서는 관련 법령의 근거규정에 따라 주민등록번호의 수집 · 이용 · 제공 등이 허용됩니다. 반면 지방자치단체나 각종 장학재단 · 단체 등은 장학금 업무를 위한 주민등록번호 수집 · 이용이 허용되지 않으므로 생년월일 등의 대체 정보를 활용할 필요가 있습니다.

상세 설명

학생에 대해 장학금을 지급하는 경우는 국가 또는 지방자치단체가 지급하는 경우, 각종 장학재단 등의 외부 단체에서 지급하는 경우, 교내 자체적으로 지급하는 경우 등으로 나눠볼 수 있습니다.

국가장학금의 경우, 「한국장학재단 설립 등에 관한 법률」에 따라 설립된 한국장학재단에서 대학생에 대한 학자금 지원, 국가장학금 지원 등의 제도를 운영 중에 있습니다. 국가장학금은 가구의 소득수준에 따라 지원되는데, 정부의 사회보장정보시스템을 통해 조사된 공적자료 및 금융재산, 금융부채 등을 파악하여 소득인정액을 산정하고 총 10개 학자금지원 구간(소득분위)를 설정한 뒤 그중 1분위~8분위에 대해 지원하고 있습니다(상세한 내용은 한국장학재단 홈페이지 www.kosaf.go.kr 참조). 따라서 국가장학금은 소득분위를 속이고 부정수급하는 경우나 지원규모를 초과하여 수혜하는 경우 등을 방지할 필요 불가피성이 있으며 이를 위해서는 해당 학생 및 부모 등의 가족관계 등록사항, 주민등록사항, 국세 관련 자료 등의 정보를 제공·활용할 것이 요구됩니다. 이를 위해서 교육부장관 및 한국장학재단은 학자금 지원신청, 자료 제출요청, 정보시스템 연계사용, 금융정보등의 제공요청 등의 사무를 위해 주민등록번호 등이 포함된 자료를 처리할 수 있도록 관련 법령에 구체적인 근거가 마련되어 있습니다(「한국장학재단 설립 등에 관한 법률」시행령 제36조의2). 따라서 국가장학금의 신청 및 심사 등을 위해서는 주민등록번호의 수집·이용·제공 등이 허용됩니다.

지방자치단체에서도 해당 지역의 거주학생 등을 대상으로 장학금 제도를 운영하는 경우가 많은데, 이 경우는 주로 조례·규칙에 근거를 두고 있으며, 해당 지역의 주민 여부(거주 여부) 등을 확인할 목적으로 신청서에 주민등록번호 기재를 요구하는 경우가 다수 있습니다. 그러나 주민등록번호 처리는 반드시 법령의 근거를 필요로 하므로, 현재로서는 지방자치단체가 장학금 지급을 위해 조례·규칙에만 근거하여 주민등록번호를 수집·이용하는 것은 허용되지 않는다고 봐야 합니다. 이 외에 각종 장학재단이나 학교 자체적으로 장학금을 심사·지급하는 경우도 마찬가지로 주민등록번호 수집·이용이 허용되지 않으므로, 생년월일 등의 대체 정보를 활용하여야 합니다.

* 대통령 소속 개인정보보호위원회는 장학금 지급을 목적으로 주민등록번호 및 사상, 종교 정보를 수집하지 않도록 관련 법령 및 지방자치단체 조례·규칙을 개선할 것을 각 소관 중앙행정기관에 권고하는 결정을 내린 바 있음(개인정보보호위원회 결정 제2015-06-11호, '15.3.23)

다만 장학금의 성격에 따라서는 해당 지역 거주 여부, 해당 가구의 소득수준 여부 등을 가족관계등록부, 주민등록등본, 재산세과세증명서 등을 접수받아 확인할 필요성도 분명히 있습니다. 따라서 이러한 경우에는 주민등록번호 뒷자리가 마스킹(***) 처리된 서류를 요청하거나, 주민등록번호 뒷자리까지 표시되어 있는 경우에는 해당 서류를 접수한 이후에 뒷자리를 삭제 처리하거나, 또는 서류를 확인만 하고 돌려주는 방법 등을 이용할 수 있습니다.

관련 법령

「한국장학재단 설립 등에 관한 법률.」

제36조의2(민감정보 및 고유식별정보의 처리) 교육부장관(법 제51조에 따라 교육부장관의 업무를 위탁받은 자를 포함한다) 및 재단은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료와 같은 영 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제50조에 따른 학자금 지원의 신청에 관한 사무
2. 법 제50조의2제1항에 따른 자료 제출의 요청에 관한 사무
3. 법 제50조의2제5항에 따른 정보시스템의 연계 사용에 관한 사무
4. 법 제50조의3제1항에 따른 금융정보등의 제공요청에 관한 사무
5. 법 제50조의4에 따른 자료요구 및 질문에 관한 사무
6. 법 제50조의5에 따른 중복 지원 방지에 관한 사무

참고자료

• 개인정보보호위원회 결정 제2015-06-11호, '장학금 관련 법령 등의 개인정보 수집 개선의 건' ('15. 3. 23)

50 저소득층 교육비 지원을 위한 주민등록번호 수집 · 이용

Q **저소득층 지원사업의 일환으로 학교 교육비 지원사업을 하는 과정에서 신청자(학생 및 학부모 등)의 주민등록번호를 수집 · 이용할 수 있는지요?**

A 국민기초생활보장의 일환으로 학교 교육급여 등 '사회복지서비스 및 급여 제공'을 신청하는 경우에는 관련 법령의 근거에 따라 신청자 및 그 가족 등의 주민등록번호를 수집 · 이용할 수 있습니다.

상세 설명

정부는 저소득층 등 생활이 어려운 사람에게 필요한 급여를 실시하여 이들의 최저생활을 보장하고 자활을 돕고 있으며, 이를 통상 '사회복지서비스 및 급여 제공'으로 부르고 있습니다. 사회복지서비스 및 급여 제공에는 생계급여, 주거급여, 의료급여, 교육급여, 해산급여, 장제급여, 자활급여 등이 있습니다(「국민기초생활 보장법」제7조). 사회복지서비스 및 급여를 받을 수 있는 사람 즉 '수급권자'는 부양의무자가 없거나 부양의무자가 있어도 부양능력이 없거나 부양을 받을 수 없는 사람으로서 소득인정액이 최저생계비 이하인 사람을 말합니다(「국민기초생활 보장법」제5조제1항).

수급권자와 그 친족, 기타 관계인은 관할 지방자치단체장에게 급여를 신청할 수 있습니다. 이때 수급권자 등은 사회복지사업 관련 법령에서 위임하여 보건복지부장관이 정하여 고시하는 '사회복지서비스 및 급여 제공(변경) 신청서' 등의 서식을 제출해야 하며, 동 서식에는 신청인 및 가족, 부양의무자 등의 성명, 주민등록번호 등을 기재하도록 하고 있습니다.

* 「사회복지사업법」 시행규칙 제33조, 「국민기초생활 보장법」 시행규칙 제42조, 「아동복지법 시행규칙」 제5조 등 사회복지사업 관련 법령은 신청서, 동의서 등의 제반 서식을 보건복지부장관이 정하여 고시하는 공통서식에 따르도록 위임하고 있으며, 이에 따라 사회복지서비스 및 급여 제공 신청에는 「사회복지사업관련 공통서식에 관한 고시」(보건복지부고시 제2014-229호, 2014. 12. 24)에서 정하는 서식이 사용됨

또한 급여신청이 접수된 경우, 지방자치단체장은 부정수급의 방지 등을 위해서 부양의무자의 유무 및 부양능력, 수급권자 및 부양의무자의 소득 · 재산, 수급권자의 근로능력 · 취업상태, 수급권자의 건강상태나 가구특성 등을 조사할 수 있고(「국민기초생활 보장법」제22조), 이를 위하여 보건복지부장관은 수급권자와 부양의무자의 동의에 따라 금융정보 · 신용정보 또는 보험정보의 제공을 금융회사등에 요청할 수도 있습니다(「국민기초생활 보장법」제23조의2).

따라서, 학교 교육비 지원(교육급여) 등 사회복지서비스 및 급여 신청과 제공을 위하여 해당 수급권자, 가족, 부양의무자 등의 주민등록번호를 수집 · 이용하는 것은 관련 법령에 구체적인 요구 · 허용 근거가 있고, 또한 수급권자 등의 소득 · 재산 등을 조사하기 위하여 주민등록번호를 수집 · 이용 · 제공해야 할 법적 근거 및 불가피성 또한 인정될 수 있습니다. 결론적으로 사회복지서비스 및 급여 신청과 제공을 위해서는 주민등록번호의 수집 · 이용이 허용됩니다.

관련 법령

「국민기초생활 보장법」

제7조(급여의 종류) ① 이 법에 따른 급여의 종류는 다음 각 호와 같다.

1. 생계급여
2. 주거급여
3. 의료급여
4. 교육급여
5. 해산급여(　　)
6. 장제급여(　　)
7. 자활급여

「국민기초생활 보장법」 시행규칙

제42조(공통서식) 제7조제2항에 따른 조건부수급자 생계급여 중지통보서, 제13조제1항에 따른 학비지급신청서, 제17조제2항에 따른 해산급여지급신청서, 제18조제1항에 따른 장제급여지급신청서, 제19조제1항 및 제4항에 따른 자금대여신청서, 자금대여 결정통지서 및 자금대여 관리카드, 제32조의4제1항에 따른 자산형성지원신청서, 제34조제1항 각호 외의 부분에 따른 급여(변경)신청서, 제34조제1항제3호 및 제35조제1항제5호에 따른 금융정보 등 제공 동의서, 제34조제3항 전단에 따른 결정통지서, 제35조제1항제4호에 따른 소득 · 재산 신고서, 제39조제1항에 따른 조사표 및 수급자관리카드와 제41조의3에 따른 보장비용 납부통지서는 사회복지관련 사업 및 서비스와 관련하여 보건복지부장관이 정하여 고시하는 공통서식에 따른다.

「사회복지사업관련 공통서식에 관한 고시」별지 서식 1호 (사회복지서비스 및 급여 제공(변경) 신청서)

[별지 제1호의서식] 〈개정 2015.1.1〉

사회복지서비스 및 급여 제공(변경) 신청서							처리기간 별도안내
□ 신규(제공)신청		□ 변경신청				□ 연장신청	
신청인	성명		주민등록번호 (외국인등록번호)		세대주와의 관계	전화번호	
	주소					휴대전화	
						전자우편	

참고자료

• 교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12.

51 대학교 증명서(재학·졸업 등) 발급 시 주민등록번호 기재

Q **대학교에서 졸업증명서와 성적증명서를 발급받았는데, 주민등록번호가 모두 노출되어 있습니다. 마스킹을 해야 하는 것 아닌가요?**

A 학교는 학적사무 처리를 위하여 학생의 주민등록번호를 처리할 수 있지만, 각종 증명서 발급시 불필요한 주민등록번호 노출이 되지 않도록 뒷자리를 마스킹하거나 생년월일로 대체하여 발급해야 합니다.

상세 설명

학교의 장은 학적부 작성·관리 등 교육의 과정 기록에 관한 사무를 수행하기 위하여 불가피한 경우 학생의 주민등록번호를 처리할 수 있도록 「고등교육법 시행령」 제73조의2 제2항에서 규정하고 있습니다.

그러나 학적사무의 일환인 각종 증명서(재학증명서, 졸업증명서, 성적증명서 등)를 발급하는 경우에는 주민등록번호의 처리가 불가피하다고 보기 어렵습니다.

따라서, 학교가 재학생 또는 졸업생에게 각종 증명서를 발급하는 경우에는 해당 증명서에 생년월일만 기재하도록 하거나 최소한 주민등록번호 뒷자리를 마스킹조치 하여 불필요한 주민등록번호의 노출이 되지 않도록 해야 합니다.

관련 법령

「고등교육법」시행령

제73조(고유식별정보의 처리)

② 학교의 장은 「교육기본법」 제16조제2항에 따른 학적부 작성·관리 등 교육의 과정 기록에 관한 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호에 따른 주민등록번호가 포함된 자료를 처리할 수 있다.

52 학교발전기금 기탁자의 주민등록번호 수집 · 이용

Q **동창회, 지역주민, 학부모 등으로부터 학교발전기금을 받는 경우가 있는데, 이 경우 기탁자의 주민등록번호를 수집 · 이용하여도 되는지요?**

A 학교발전기금을 기탁받아 조성함에 있어서는 「초 · 중등교육법」등 관련 법령에 명시적인 근거가 있으므로 기탁자의 주민등록번호를 수집 · 이용할 수 있습니다.

상세 설명

학교발전기금이란 학교의 교육활동을 지원하기 위하여 기부자가 기부한 금품, 학부모 등으로 구성된 학교 내 · 외의 조직 · 단체 등이 그 구성원으로부터 자발적으로 조성하거나 구성원 외의 자로부터 모금한 금품 등을 말합니다(「초 · 중등교육법」제33조, 동법 시행령 제64조). 학교발전기금은 학교교육시설의 보수 및 확충, 교육용 기자재 및 도서의 구입, 학교체육활동 기타 학예활동의 지원, 학생복지 및 학생자치활동의 지원 목적 등 학교발전기금 운용계획에 의거 조성목적의 범위 내에서 사용하여야 하며, 반면 학교회계 부족분에 충당하거나 일반 수용비성 경비에 사용하는 경우, 교직원의 각종 수당(인건비) · 여비 · 연수비 · 회식비 등에 사용하는 경우, 각종 협의회비 · 간담회비, 선물비, 경조사비 등 업무추진비에 사용하는 경우 등은 제한됩니다.

학교발전기금의 기탁자는 자신의 성명, 주민등록번호, 주소, 전화 등 인적사항, 기금이나 물품 · 시설의 기탁 명세, 사용 용도 등을 기재한 기탁서를 제출해야 합니다(「초 · 중등교육법」시행규칙 별지 제27호 서식). 한편 학교발전기금을 기탁받은 학교(발전기금회계출납원)는 기금을 수납하고 영수증을 교부해야 하며 금융기관 또는 체신관서를 통해 접수하는 경우에도 발전기금 기부서 영수증을 교부하는데, 이 영수증은 「소득세법」 및 「법인세법」에 따른 기부금 납부증명서로 사용될 수 있습니다(교육부, '학교발전기금의 조성 · 운용 및 회계관리요령 참조). 또한 향후에 기탁자가 「소득세법」등에 따라 기탁자 소득공제를 위하여 기부금영수증을 요구하는 경우에도 이의 발급을 위하여 기탁자의 주민등록번호가 요구됩니다.

따라서, 학교가 학교발전기금 기탁자의 주민등록번호를 수집 · 이용하는 것은 「초 · 중등교육법」등 관련 법령에 구체적인 요구 · 허용 근거가 있으므로, 기탁자의 주민등록번호를 수집 · 이용하는 것이 허용됩니다.

관련 법령

「초 · 중등교육법」

제33조(학교발전기금) ① 제31조에 따른 학교운영위원회는 학교발전기금을 조성할 수 있다.

② 제1항에 따른 학교발전기금의 조성과 운용방법 등에 필요한 사항은 대통령령으로 정한다.

「초 · 중등교육법」 시행령

제64조(학교발전기금) ① 법 제33조의 규정에 의한 학교발전기금(이하 "발전기금"이라 한다)은 다음 각호의 방법에 의하여 조성한다.

1. 기부자가 기부한 금품의 접수

2. 학부모 등으로 구성된 학교내·외의 조직·단체 등이 그 구성원으로부터 자발적으로 갹출하거나 구성원외의 자로부터 모금한 금품의 접수

「초 · 중등교육법」 시행규칙 별지 제27호 서식 **(학교발전기금 기탁서)**

학교발전기금 기탁서

1.기탁자 인적사항

성명	
주민등록번호	
주소	
전화	

참고자료

- 교육부, 「교육부 개인정보보호 업무사례집」, 2014. 12.
- 교육부, 「학교발전기금의 조성 · 운용 및 회계관리요령」, 2012. 7.

제 8 장

기타 사례

제8장 기타 사례

53 동호회 회원의 주민등록번호 수집 · 이용

Q **저희 산악 동호회에서 소속 회원들의 신원확인과 친목 관리를 위하여 회원 명단에 주민등록번호를 기재하고 있습니다. 문제가 없는지요?**

A 동호회, 동창회 등 친목도모 단체라 하더라도 다른 법령의 근거규정이 없는한 회원들의 주민등록번호를 수집 · 이용하는 것은 허용되지 않습니다.

상세 설명

「개인정보 보호법」은 동호회, 동창회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 일부 조항의 적용을 면제하고 있습니다. 친목 도모를 위한 단체에 적용이 배제되는 조항은 제15조(개인정보의 수집 · 이용), 제30조(개인정보 처리방침의 수립 및 공개), 제31조(개인정보 보호책임자의 지정)입니다(「개인정보 보호법」제58조제3항).

따라서 동호회, 동창회 등 친목 도모를 위한 단체가 이 이외의 개인정보 처리를 하는 경우에는 「개인정보 보호법」의 적용을 받게 됩니다. 예를 들어 친목 도모를 위한 단체가 회원들의 개인정보를 제3자에게 제공하거나 목적 외로 이용하고자 하는 경우에는 법 제17조 및 제18조에 따른 요건을 반드시 갖추어야 하며, 그렇지 않을 경우에는 법률에서 정한 처벌이 과해질 수도 있습니다.

이는 주민등록번호 처리금지 및 법정주의를 규정한 법 제24조의2에 대해서도 마찬가지입니다. 즉 즉 동호회, 동창회 등 친목 도모를 위한 단체는 원칙적으로 주민등록번호의 처리가 금지되며, 다만 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우, 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정하는 경우 등에만 예외적으로 주민등록번호의 처리가 허용됩니다.

따라서 단순히 동호회나 동창회 소속 회원들의 신원확인과 친목 도모를 위한 목적으로 주민등록번호를 수집 · 이용하는 것은 법령의 구체적 근거가 있는 경우는 아니므로, 이 경우에는 주민등록번호의 수집 · 이용이 금지된다 하겠습니다.

관련 법령

「개인정보 보호법」

제58조(적용의 일부 제외) ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

54 교회 교인명부에 주민등록번호 기재

Q **저희 교회에서는 신도가 처음 방문한 경우 성명, 주민등록번호, 주소, 연락처 등을 확인하여 교인명부에 기재하고 있습니다. 이러한 방식이 문제가 될 수 있는지요?**

A 원칙적으로 종교단체가 선교 등의 종교활동을 위하여 개인정보를 처리하는 경우는 개인정보 보호법 상 개인정보 수집 · 이용, 제공 등의 규제를 받지않습니다. 다만, 이러한 경우에도 주민등록번호가 반드시 필요한 경우가 아니라면 가급적 주민등록번호를 수집하지 않는 것이 바람직합니다. 이와 별도로, 기부금영수증 발급에 필요한 주민등록번호는 관련법령에 의거하여 수집할 수 있습니다.

상세 설명

「개인정보 보호법」은 언론, 종교단체, 정당이 각각 취재 · 보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집 · 이용하는 개인정보에 대해서는「개인정보 보호법」의 제3장부터 제7장까지 적용하지 않도록 규정하고 있습니다(「개인정보 보호법」제58조제1항). 이는 개인정보보호를 지나치게 강조하면 헌법에서 보장하고 있는 표현의 자유(언론의 자유), 종교의 자유 등 다른 기본권이 위축되는 결과를 초래할 수도 있으므로, 개인정보를 적절히 보호하면서 다른 헌법적 가치와의 균형을 위하여 일정한 유형의 개인정보 처리에 대해서는「개인정보 보호법」의 일부 적용을 면제할 필요가 있기 때문입니다.

종교단체의 '선교 등 고유목적을 달성하기 위한 활동'에는 1) 교단정리, 교단 내부규율 정리, 교역자 신상관리, 소식지 제작, 각종 회의소집, 교단 홈페이지 관리 등 종교단체의 교단유지 업무, 2) 종교단체의 교리를 전파하거나 전쟁 · 재해를 입은 주민의 재건과 화해를 위한 선교활동, 3) 종교 교리를 전달하고 종교를 전파할 목적으로 행하는 교육 등이 이에 해당합니다(행정자치부,「개인정보 보호법령 및 지침 · 고시 해설」, 2011. 12 참조).

따라서, 주민등록번호 처리금지 및 법정주의를 규정한「개인정보 보호법」제24조의2는 종교단체가 선교 등 고유목적을 달성하기 위하여 주민등록번호를 처리하는 경우에는 적용되지 않습니다. 한가지 유의할 점은 종교단체가 처리하는 모든 활동에 대해「개인정보 보호법」제3장에서 제7장의 규정이 적용 제외되는 것이 아니며, 어디까지나 '선교 등 고유목적 달성'에 필요한 범위 안에서만 적용되어야 합니다. 다만, 종교단체의 선교 등 고유목적 달성을 위한 경우라 하더라도 실제로 주민등록번호의 처리가 반드시 필요 불가피한 경우는 많지 않을 것으로 여겨집니다. 따라서 질의와 같이 교회에서 교인명부 등을 작성 · 관리하는 경우에는 가급적 주민등록번호를 삭제하고 생년월일 등의 정보로 대체하는 것이 바람직할 것입니다.

한편, 이와 별개로 교회, 성당, 사찰 등에서는 신도들의 헌금, 교무금, 시주금 등의 명목으로 기부금을 받는 경우가 많습니다. 이 경우 신도들이 「소득세법」에 따라 연말세액공제를 받기 위하여 기부금영수증 발급을 원하는 때에는 이를 발급하고 기부금영수증 발급명세를 작성·관리·보관할 의무가 있으므로(「소득세법」제59조의4제4항, 제160조의3 등 참조), 이에 필요한 범위 내에서는 기부금을 낸 신도들의 주민등록번호를 수집·이용할 수 있습니다.

관련 법령

「개인정보 보호법」

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보

「소득세법」

제59조의4(특별세액공제) ④ 거주자(사업소득만 있는 자는 제외하되, 제73조제1항제4호에 따른 자 등 대통령령으로 정하는 자는 포함한다)가 해당 과세기간에 지급한 기부금[제50조제1항제2호 및 제3호에 해당하는 사람(다른 거주자의 기본공제를 적용받은 사람은 제외한다)이 지급한 기부금을 포함한다]이 있는 경우 다음 각 호의 기부금을 합한 금액에서 사업소득금액을 계산할 때 필요경비에 산입한 기부금을 뺀 금액의 100분의 15(해당 금액이 3천만원을 초과하는 경우 그 초과분에 대해서는 100분의 25)에 해당하는 금액(이하 이 조에서 "기부금 세액공제액"이라 한다)을 해당 과세기간의 합산과세되는 종합소득산출세액(필요경비에 산입한 기부금이 있는 경우 사업소득에 대한 산출세액은 제외한다)에서 공제한다. 이 경우 제1호의 기부금과 제2호의 기부금이 함께 있으면 제1호의 기부금을 먼저 공제하되, 2013년 12월 31일 이전에 지급한 기부금을 2014년 1월 1일 이후에 개시하는 과세기간에 이월하여 소득공제하는 경우에는 해당 과세기간에 지급한 기부금보다 먼저 공제한다.

1. 법정기부금
2. 지정기부금. 이 경우 지정기부금의 한도액은 다음 각 목의 구분에 따른다.

가. 종교단체에 기부한 금액이 있는 경우 (이하 생략)

55 주택조합의 조합원 명부에 주민등록번호 기재

Q **주택조합의 조합원 명부에 주민등록번호를 기재해야 하는지요? 만약 조합원이나 토지등 소유자가 조합원명부의 공개·열람 등을 요구하는 경우에는 주민등록번호도 공개해야 하는 것인지 알고 싶습니다.**

A 주택조합의 조합원 명부에는 원칙적으로 조합원의 성명, 생년월일, 주소, 전화번호 등만 기재하며 주민등록번호는 기재하지 않습니다. 따라서 조합원등이 조합설립추진위원회 위원장이나 사업시행자에게 조합원명부의 공개 · 열람 · 복사 등을 요구하는 경우에는 주민등록번호가 포함되지 않은 정보로 공개하여야 합니다.

상세 설명

주택조합이란 많은 수의 구성원들이 주택을 마련하거나 리모델링하기 위하여 결성하는 조합을 말합니다. 여기에는 지역주택조합, 직장주택조합, 리모델링주택조합이 있습니다(「주택법」제2조제11호). 지역이나 직장 등 많은 수의 구성원들이 주택을 마련하거나 리모델링하기 위하여 주택조합을 설립하려는 경우에는 관할 시장 · 군수 · 구청장의 인가를 받아야 하며, 인가받은 내용을 변경하거나 주택조합을 해산하려는 경우에도 역시 인가가 필요합니다(「주택법」제32조).

주택조합의 설립 · 변경 · 해산의 인가를 받으려는 자는 인가신청서를 관할 시장 · 군수 · 구청장에게 제출하여야 하는데, 여기에는 '조합원 명부' 등의 서류가 첨부되어야 합니다(「주택법」시행령 제37조, 시행규칙 별지 제23호 서식). 이전에는 조합원 명부 서식에 조합원의 성명, 주민등록번호, 주소, 전화번호 등을 기재하도록 하였으나, 현행 「주택법」에 따른 조합원 명부 서식에는 성명, 생년월일, 주소, 전화번호 등을 기재하고 주민등록번호는 기재하지 않도록 하고 있습니다. 따라서 조합원 명부에는 주민등록번호를 기재하여야 할 구체적인 법령 상의 요구·허용 근거가 없으므로 주민등록번호를 기재하여서는 안됩니다.

* 주택조합 조합원이 될 수 있는 자는 주택 미소유 또는 주거전용면적 85제곱미터 이하 주택 1채 소유한 세대주 여부, 조합설립인가신청일 현재 6개월 이상 거주 여부 등 조합원 자격에 부합하여야 하며(「주택법」시행령 제38조), 이를 위하여 시장·군수·구청장은 조합원 자격의 해당여부 등을 확인하기 위해 국토교통부장관에게 주택전산망에 의한 전산검색을 의뢰하여 확인할 수 있음(「주택법」 시행규칙 제18조제3항)

따라서 조합원이나 토지등 소유자가 주택조합 해산동의서 징구 등의 목적으로 조합설립추진위원회 위원장이나 사업시행자에게 조합원 명부를 요청하고, 반면 조합등은 공개지연, 거부, 부실제공 등으로 상호 다툼과 민원이 발생하는 사례가 많이 있어 왔습니다. 이러한 문제를 해결하기 위해 2012. 2. 1 「도시 및 주거환경정비법」을

개정하여, 조합설립추진위원회 또는 사업시행자는 정비사업 시행에 관한 서류와 관련 자료(토지등소유자 명부, 조합원 명부 등)를 조합원, 토지등소유자가 열람 · 복사 요청을 한 경우에는 주민등록번호가 포함되지 않은 정보를 공개하여야 합니다.

관련 법령

「주택법」 시행령

제37조(주택조합의 설립인가 등) ① 법 제32조제1항에 따라 주택조합의 설립·변경 또는 해산의 인가를 받으려는 자는 인가신청서에 다음 각 호의 구분에 따른 서류와 해당 주택건설대지의 100분의 80 이상의 토지에 대한 토지사용승낙서(지역·직장주택조합의 경우만 해당한다)를 첨부하여 주택조합의 주택건설대지(리모델링주택조합의 경우에는 해당 주택의 소재지를 말한다. 이하 같다)를 관할하는 특별자치시장·특별자치도지사·시장·군수·구청장(이하 "시장·군수·구청장"이라 한다)에게 제출하여야 한다.

1. 설립인가의 경우

가. 지역·직장주택조합의 경우

(4) 조합원 명부 (이하 생략)

「주택법」 시행규칙 별지 제23호 서식 (주택조합 설립 · 변경 · 해산인가 신청서)

조합원 현황			*해산인가의 경우에는 적지 않습니다.			
일련번호	성명	생년월일	주소	전화번호	적격 여부	비고

참고자료

- 서울특별시, '조합원명부 등 공개 업무처리기준', 2013. 9.

행정자치부 KISA 한국인터넷진흥원

주민등록번호 처리기준
분야별 상담사례집