발간물등록번호 | KISA-GD-2020-0029

개인정보 영향평가 수행안내서

2020. 12.

개인정보보호위원회

KISA 한국인터넷진흥원

CONTENTS

PART 01 총론

6 제1절 개인정보 영향평가 개요
1. 개념
2. 목적 및 필요성
3. 평가 대상
4. 평가 시기
5. 평가 수행 주체
6. 평가 수행 체계

10 제2절 용어정의 및 추진근거
1. 용어정의
2. 추진근거

12 제3절 개인정보 영향평가 수행절차 요약

PART 02 영향평가 수행절차

15 제1절 영향평가 사전준비 단계
1. 사업계획의 작성
1.1. 영향평가 필요성 검토
1.2. 사전평가 수행
1.3. 사업계획서 작성
2. 영향평가 기관 선정
2.1. 제안요청서 작성 및 사업발주
2.2. 영향평가 기관 선정

21 제2절 영향평가 수행단계
1. 영향평가 수행계획 수립
1.1. 영향평가 수행계획 수립
1.2. 영향평가팀 구성방안 협의
1.3. 영향평가팀 역할 정의
1.4. 영향평가팀 운영계획 수립

2. 평가자료 수집
2.1. 내부 정책자료 분석
2.2. 외부 정책자료 분석
2.3. 대상시스템 관련 자료 분석
3. 개인정보 흐름 분석
3.1. 개인정보 처리 업무 현황 분석
3.2. 개인정보 처리 업무 흐름도 작성
3.3. 개인정보 흐름표 작성
3.4. 개인정보 흐름도 작성
3.5. 정보시스템 구조도 및 정보보호 시스템 목록 작성
4. 개인정보 침해요인 분석
4.1. 평가항목 구성
4.2. 개인정보 보호조치 현황파악
4.3. 개인정보 침해요인 도출
4.4. 개인정보 위험도 산정
5. 개선계획 수립
5.1. 개선사항 도출
5.2. 개선계획 수립
6. 영향평가서 작성

77 제3절 이행단계
1. 이행점검
1.1. 개선사항 반영점검
1.2. 개선계획 이행점검

부록

80 부록1. 개인정보 영향평가서 양식
122 부록2. 개인정보 영향평가 항목(요약)
130 부록3. 개인정보 영향평가 항목(평가표)
462 부록4. 개인정보 영향평가 FAQ

PART

01

제1장 **총론**

제1절 개인정보 영향평가 개요
제2절 용어정의 및 추진근거
제3절 개인정보 영향평가 수행절차 요약

제1장

총론

제1절 개인정보 영향평가 개요

1. 개념

● **개인정보 영향평가(이하 영향평가)**

- 개인정보파일을 운용하는 새로운 정보시스템의 도입이나 기존에 운영 중인 개인정보 처리시스템의 중대한 변경 시
- 시스템의 구축·운영·변경 등이 개인정보에 미치는 영향(impact)을 사전에 조사·예측·검토하여 개선방안을 도출하고 이행여부를 점검하는 체계적인 절차

2. 목적 및 필요성

● 개인정보 처리가 수반되는 사업 추진시 해당 사업이 개인정보에 미치는 영향을 사전에 분석하고 이에 대한 개선방안을 수립하여 개인정보 침해사고를 사전에 예방

3. 평가 대상

● 일정규모 이상의 개인정보를 전자적으로 처리하는 개인정보파일을 구축·운영 또는 변경하려는 공공기관은 「개인정보 보호법」(이하 "법"이라 한다) 제33조 및 「개인정보 보호법 시행령」 (이하 "영"이라 한다) 제35조에 근거하여 영향평가를 수행

- **(5만명 조건)** 5만명 이상의 정보주체의 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- **(50만명 조건)** 해당 공공기관의 내부 또는 외부의 다른 개인정보파일과 연계하려는 경우로서, 연계 결과 정보주체의 수가 50만 명 이상인 개인정보파일
- **(100만명 조건)** 100만 명 이상의 정보주체 수를 포함하고 있는 개인정보파일

※ 현시점 기준으로 영향평가 대상은 아니나 가까운 시점(1년 이내)에 정보주체의 수가 법령이 정한 기준 이상이 될 가능성이 있는 경우, 영향평가를 수행할 것을 권고

- **(변경 시)** 영제35조에 근거하여 영향평가를 실시한 기관이 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우, 변경된 부분에 대해서는 영향평가를 실시

※ 법령상 규정된 대상시스템이 아니더라도 대량의 개인정보나 민감한 개인정보를 수집·이용하는 기관은 개인정보 유출 및 오·남용으로 인한 사회적 피해를 막기 위해 영향평가 수행 가능

개인정보파일 및 개인정보처리시스템 정의

개인정보파일

(정의) 개인정보파일은 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다. 개인정보파일은 데이터베이스 등 전자적인 형태뿐만 아니라 수기(手記)문서 자료도 포함하지만, 영향평가의 대상이 되는 개인정보파일은 전자적으로 처리할 수 있는 것에 한정되어 있으므로 일반적으로 종이 등의 문서에 수기로 기록된 개인정보 문서는 대상에서 제외된다. 단, 종이로 기록된 개인정보 문서가 PDF 등의 전자적인 매체로 변환될 경우 해당 PDF 파일 등은 평가의 대상이 될 수 있다.

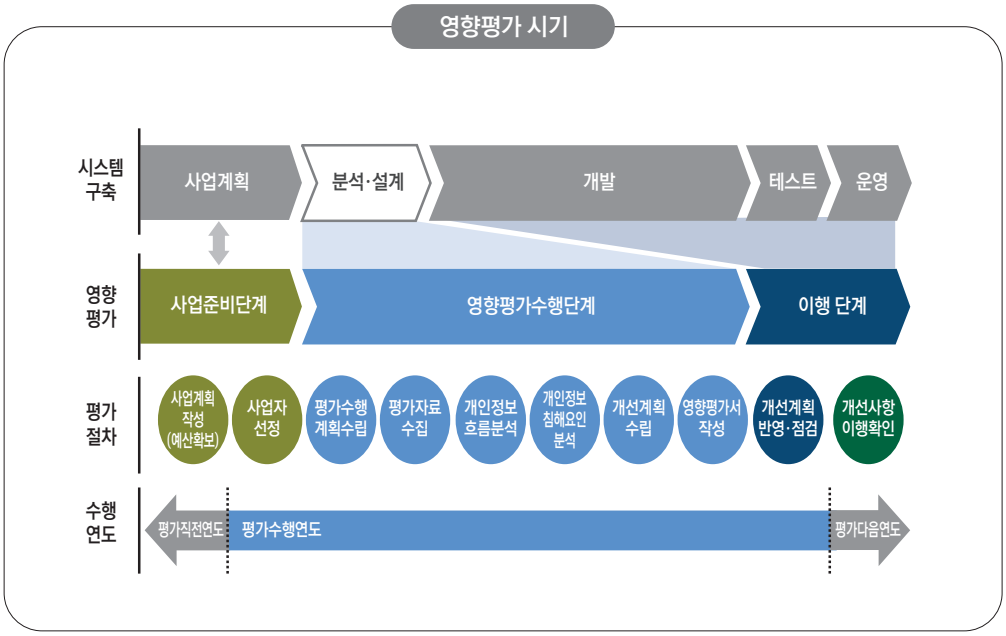
개인정보 처리시스템

(정의) 개인정보처리시스템이란 데이터베이스 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다. 개인정보처리시스템은 일반적으로 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말한다. 다만, 개인정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있으며 작게는 한 대의 서버에서부터 크게는 수백 대의 서버 및 DBMS를 운영하는 것까지 다양한 규모를 가지고 있다. 영향평가에서는 개인정보처리시스템 내의 개인정보파일을 안전하게 보호하기 위하여 필요한 기술적·관리적 및 물리적 안전조치가 적절하게 적용되었는지 여부를 비롯하여 개인정보의 수집, 저장, 이용, 제공, 파기 등 생명주기 상에 관련 법규를 준수하고 정보주체의 권리를 제대로 보장하고 있는지를 확인하고 문제점이 있는 경우 개선방안을 제시하게 된다.

공공기관의 범위(법 제2조제6호)

- 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
- 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
  1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
  2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
  3. 「지방공기업법」에 따른 지방공사 및 지방공단
  4. 특별법에 의하여 설립된 특수법인
  5. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교
- 단, 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따름 (「개인정보 보호법」 제33조 제7항)

4. 평가 시기



4.1. 시스템을 신규 구축 또는 기존 시스템을 변경하는 경우

- 개인정보처리시스템을 신규로 구축 하거나 기존 시스템을 변경하려는 기관은 사업계획 단계에서 영향평가 의무대상 여부를 파악하여 예산을 확보한 후, 대상 시스템의 설계 완료 전에 영향평가를 수행해야 함. 또한 영향평가 결과는 시스템 설계·개발 시 반영해야 함(「개인정보 영향평가에 관한 고시」 제9조의2)

4.2. 기 구축되어 운영 중인 시스템의 경우

- 개인정보처리시스템을 기 구축·운영 중, 아래의 경우 추가적으로 영향평가 수행 가능
  - 수집·이용 및 관리상에 중대한 침해위험의 발생이 우려되는 경우
  - 전반적인 개인정보 보호체계를 점검하여 개선하기 위한 경우

5. 평가 수행 주체

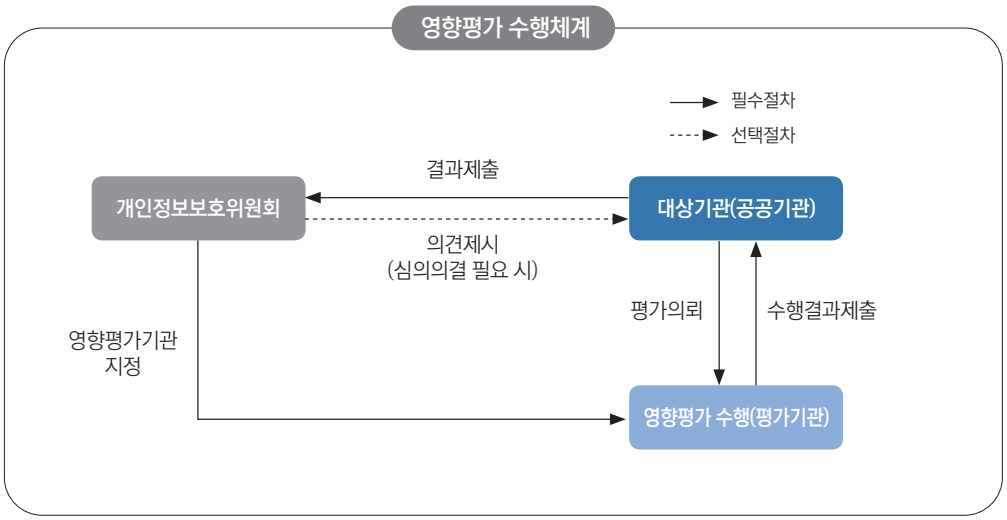
- 공공기관은 개인정보보호위원회가 지정한 영향평가기관에 평가를 의뢰하여 수행

  ※ 영향평가기관에 대한 정보는 개인정보보호 포털(privacy.go.kr)에서 확인 가능

6. 평가 수행 체계

- 영향평가는 개인정보보호위원회가 지정한 영향평가기관에 의뢰하여 영향평가를 수행하고 그 결과를 사업 완료 후 2개월 이내에 개인정보보호위원회에 제출*
  - 개인정보보호위원회는 심의·의결을 거쳐 해당 사업에 대한 의견 제시 가능

* 개인정보보호 종합지원시스템(https://intra.privacy.go.kr)에 등록



제2절 용어정의 및 추진근거

1. 용어정의

개인정보	'개인정보'란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말하며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보가 포함된다. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려해야 한다. 또한 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 가명처리한 정보 즉, 가명정보도 개인정보에 포함됨
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 행위(「개인정보 보호법」 제2조제2호)
정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람(「개인정보 보호법」 제2조제3호)
개인정보파일	개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)(「개인정보 보호법」 제2조제4호)
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등(「개인정보 보호법」 제2조제5호)
영상정보처리기기	일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치(「개인정보 보호법」 제2조제7호)
민감정보	사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종정보 또는 민족정보(「개인정보 보호법」 제23조제1항제1호제2호 및 동법 시행령 제18조)
고유식별정보	법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 의미(「개인정보 보호법」 시행령 제19조)

개인정보취급자	개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말함(표준 개인정보 보호지침 제2조 제6호) ※ 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면, 정규직, 비정규직, 하도급, 시간제 등 모든 근로 형태를 불문하며, 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함(개인정보 보호법령 및 지침·고시 해설 제28조)
개인정보처리 시스템	데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(개인정보의 안전성 확보조치 기준 제2조 제10호)
위험도 분석	개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위(개인정보의 안전성 확보조치 기준 제2조 제11호)
개인정보 영향평가 (이하 영향평가)	법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가(「개인정보 영향평가에 관한 고시」 제2조제1호)
대상기관	영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관 (「개인정보 영향평가에 관한 고시」 제2조제2호)
개인정보 영향평가기관 (이하 평가기관)	영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 보호위원회가 지정한 기관(「개인정보 영향평가에 관한 고시」 제2조 제3호)
대상시스템	영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템 (「개인정보 영향평가에 관한 고시」 제2조 제4호)

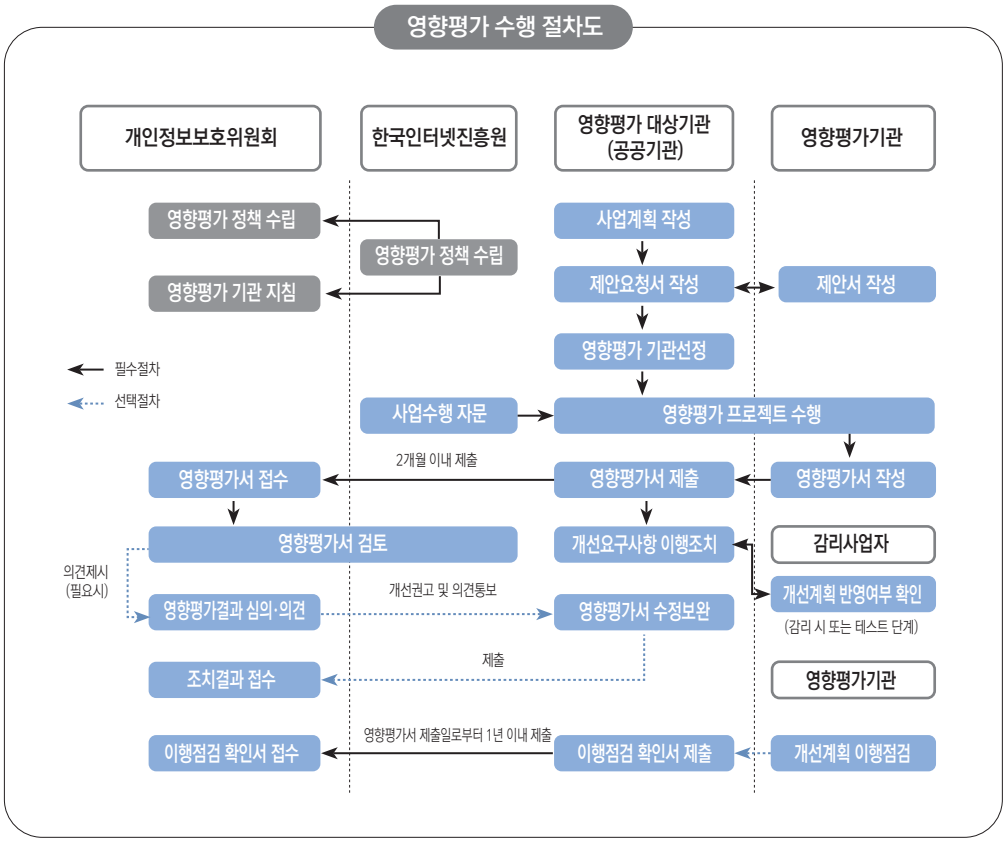
2. 추진근거

- 개인정보 보호법 제33조(영향평가)
- 개인정보 보호법 시행령 제35조(영향평가의 대상)
- 개인정보 보호법 시행령 제36조(영향평가 시 고려사항)
- 개인정보 보호법 시행령 제37조(평가기관의 지정 및 지정취소)
- 개인정보 보호법 시행령 제38조(영향평가의 평가기준 등)
- 개인정보 처리 방법에 관한 고시(개인정보보호위원회고시 제2020-7호) 제3조(개인정보 보호업무 관련 장부 및 문서 서식) [시행 2020.8.11.]
- 개인정보 영향평가에 관한 고시(개인정보보호위원회고시 제2020-4호) [시행 2020.8.11.]

제3절 영향평가 수행 절차 요약

- 영향평가 사업은 직전연도에 예산을 확보하고, 당해연도에 평가기관을 선정하여 대상기관과 평가기관이 협업을 통해 영향평가서를 완성
  - 영향평가서는 최종 제출받은 날로부터 2개월 이내에 개인정보보호위원회에 제출
  - 영향평가서를 제출한 날로부터 1년 이내에 이행점검 확인서를 개인정보보호위원회에 제출

※ 제출방법 : 개인정보보호 종합지원시스템(https://intra.privacy.go.kr)에 등록



PART

02

제2장

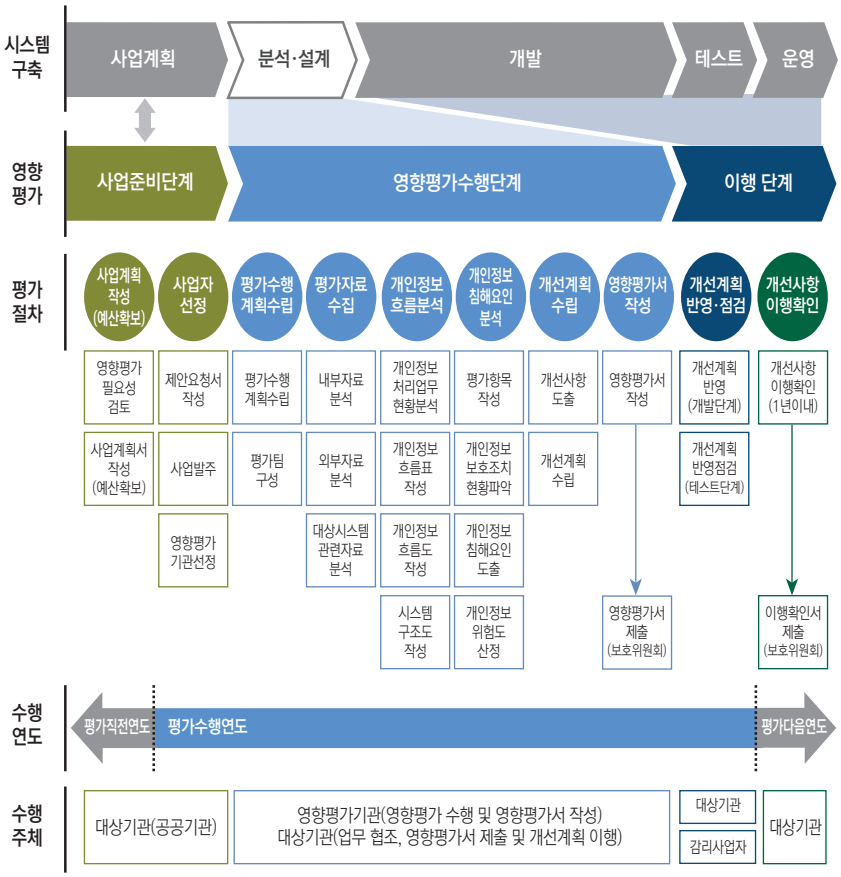
영향평가 수행절차

제1절 영향평가 사전준비 단계
제2절 영향평가 수행단계
제3절 이행단계

영향평가 사업은 사전준비 단계, 수행단계, 이행단계 등 3단계로 구성

영향평가 사전준비 단계	영향평가 사업계획을 수립하여 신규 또는 변경 사업 추진 시 타당성 검토 후 조직 내 영향평가 협력 조직 구성 및 영향평가 수행 방향을 수립하여야 한다. 이후 필요한 예산 및 지원 인력 등의 자원을 확보하고 평가기관을 선정, 선정된 평가기관이 포함된 영향평가팀을 구성
영향평가 수행단계	선정된 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성
이행 단계	영향평가서의 침해요인에 대한 개선계획을 반영하고 이를 점검

영향평가 절차



제2장

영향평가 수행절차

제1절 영향평가 사전준비 단계

1. 사업계획의 작성

1.1. 영향평가 필요성 검토

목 표	구축 또는 변경하고자 하는 정보화사업(정보시스템)에 대해 영향평가 필요성 여부 판단
개 요	정보화사업을 추진하는 과정에서 개인정보의 신규 수집·이용·연계·제공 또는 처리절차상 변경 등으로 영향평가 대상이 되는지에 대해 영 제35조에 근거하여 판단
수행주체	대상사업 주관 부서
참고자료	사업계획서, 제안요청서(RFP) 등
산 출 물	영향평가 필요성 검토서 (영 제35조에 근거하여 작성)

- 영 제35조에 근거하여 특정 정보주체 수 이상(제1장 제1절 평가대상 참조)의 개인정보를 전자적으로 처리하는 공공기관은 영향평가를 의무적으로 수행
  - 영향평가를 실시하는 3가지 유형
    ① 개인정보파일을 신규 구축·운용 하려는 경우
    ② 기 운용 중인 개인정보파일의 수집, 보유, 이용·제공, 파기 등 처리절차를 변경하거나 개인정보 검색체계 등 개인정보파일 운용체계를 변경하려는 경우
    ③ 개인정보파일을 타 시스템과 연계·제공하려는 경우
- 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 자율적으로 판단하여 영향평가를 하기 위하여 적극 노력 (「개인정보 보호법」 제33조 제8항)

개인정보파일의 운용체계 변경 예시

- 기 수집된 개인정보파일의 처리절차가 변경되는 경우는 개인정보 처리시스템의 추가·변경 또는 개인정보 수집 경로, 처리절차의 확대·변경하는 경우로 구분
  - 개인정보처리시스템을 추가·변경하려는 경우 : 데이터베이스시스템 혹은 응용프로그램 등의 개인정보 처리시스템이 노후하여 이를 신규로 구축하거나 기능을 고도화 하는 경우
    ※ 예) 교육청이 해당관할 내 학교소속 학생들의 진로상담을 위해 기존에 운용하던 정보 시스템을 신규로 구축하는 경우
  - 개인정보 수집 경로 및 처리절차를 확대·변경하려는 경우 : 기존 개인정보파일의 수집경로가 온라인에서 오프라인까지 확대되거나, 수집·보유·이용·제공 파기 등 개인정보 처리절차가 변경되는 경우
    ※ 예) ○○증명서 발급을 위한 개인정보 수집을 기존 각 구청에서 전국 읍·면사무소(주민센터)로 확대하는 경우
- 기관 내부의 다른 정보시스템과 개인정보처리시스템을 새롭게 연계하거나, 기존 연계방식 또는 연계하는 데이터를 변경하는 경우
- 개인정보의 수집 방법을 기존 정보주체로부터 직접 수집하는 방식에서 간접 수집 방식으로 변경하는 경우
- 수집·처리되는 개인정보의 항목이 추가되거나 변경된 경우 또는 개인정보 수집·이용 목적에 변경이 발생하는 경우
- 기존 정보시스템에 신기술을 적용하는 등의 새로운 활용법을 채택함으로써 기존에 수집되거나 향후 수집될 정보가 본인 확인이 가능한 형태로 변경되는 등 시스템 상에 중대한 변화가 발생하는 경우
- 신규 또는 추가로 구축된 시스템이 개인정보 DB에 대한 접근을 관리 또는 통제하기 위해 사용되는 보안체계에 중대한 변화를 초래하는 경우
- 사업의 서비스 이용과정에서 생성되는 정보를 기존에 수집한 개인정보와 결합시킴으로써 정보주체의 프라이버시에 영향을 미칠 수 있는 이차적인 정보가 생성되는 경우

※ 기존 업무처리 절차나 개인정보보호 체계의 변경이 없는 단순 노후장비 교체, 운영·유지보수 사업의 경우 영향평가 대상에서 제외할 수 있다.

외부기관과의 연계 예시

- 기존에 보유하고 있는 개인정보파일을 외부기관과 연계하는 경우, 새로운 개인정보파일을 연계하는 경우와 기존 연계 절차를 변경하는 경우로 구분
  - 외부기관의 요청 또는 법률 근거에 의해 개인정보파일을 외부기관과 연계·연동 혹은 이관하는 경우
    ※ 예) 각 시·군청에서 관리하고 있는 학비지원 대상자를 상위기관인 도청에서 추가로 취합·관리하기 위해 학비지원 대상자 현황을 일정주기로 연계하여 자료를 갱신하고자 하는 경우
  - 기존 외부기관과의 개인정보파일 연계·연동 절차를 변경하려는 경우
    ※ 예) 각 시·군청에서 관리하고 있는 자원봉사자를 상위기관인 도청에서 취합·관리하고 있는데, 취합하는 자원봉사자의 개인정보가 추가되거나, 취합절차가 기존 공문 및 명단 우편발송에서 실시간 시스템 연동으로 변경하려는 경우

1.2. 사전평가 수행(선택사항)

- 대상기관은 영향평가기관을 통해 영향평가를 수행하기 전에 영향평가 자율수행 프로그램(privacy.go.kr)을 통해 맛보기 기능 활용 가능
  - 영향평가 맛보기 기능은 대상시스템 및 영향평가 절차 등에 대한 이해도를 높일 수 있고, 사업발주 시 평가기관에 대한 사업관리 등에 활용 가능

1.3. 사업계획서 작성

- 영향평가 사전준비 단계로 영향평가 사업계획서를 작성하고, 영향평가 예산 확보를 위해 사업계획에 포함

사업계획서 및 제안요청서 목차(예시)

사업계획서 목차		제안요청서 목차	
I. 사업개요	1. 사업개요	1. 사업개요	I. 사업 안내
	2. 추진배경 및 필요성	2. 추진배경 및 필요성	
	3. 사업범위	3. 사업범위	
	4. 기대효과	4. 기대효과	
II. 대상업무현황	1. 업무현황	1. 업무현황	II. 대상업무현황
	2. 정보시스템 현황	2. 정보시스템 현황	
	3. 선진사례	3. 선진사례	
	4. 문제점 및 개선과제	4. 문제점 및 개선과제	
III. 사업추진계획	1. 추진목표	1. 추진목표	III. 사업추진계획
	2. 추진전략	2. 추진전략	
	3. 추진체계 및 역할	3. 추진체계 및 역할	
	4. 추진일정	4. 추진일정	
IV. 사업내용	1. 주요 사업내용	1. 주요 사업내용	IV. 제안요청개요
	2. 세부 사업내용	2. 세부 사업내용	
V. 소요자원 및 예산		3. 용역산출물	
VI. 기타지원요건	1. 교육지원 요건	4. 보안요건	
	2. 기술지원 요건	5. 기타지원요건	
	3. 유지보수 요건		

2. 영향평가 기관 선정

목 표	기관의 영향평가를 수행할 평가기관을 선정
개 요	개인정보보호위원회가 지정한 영향평가기관을 대상으로 평가기관을 선정 제안요청서를 작성하고, 사업발주 후 평가기관 중 적합한 기관을 선정
수행주체	사업주관부서 (영향평가 주관부서)
참고자료	각 기관 업무분장
산 출 물	제안요청서(대상기관), 제안서(영향평가기관)

2.1. 제안요청서 작성 및 사업발주

● 사업계획서에 기반하여 영향평가 사업발주를 위한 제안요청서를 작성

사업발주 시 주의사항

● 제안요청서 작성 시 영향평가 대상 시스템의 설계 완료 전에 영향평가를 수행하도록 일정 계획을 제시하여야 하며, 영향평가 개선계획의 반영여부를 감리 또는 테스트 단계에서 확인할 수 있도록 사업 발주 필요

- 대상 시스템의 설계 완료 전에 영향평가 수행
- 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인해야 하므로, 정보시스템 감리 사업발주 시 관련 요건을 포함하여 발주 필요. 단, 감리를 수행하지 않은 경우에는 정보시스템 테스트 단계에서 영향평가 개선계획의 반영여부를 확인
- 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행 현황을 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회에 제출해야 하므로, 필요시 관련 요구 사항을 제안요청서에 포함

● 시스템 구축 사업의 일부분으로써 영향평가를 포함하여 발주할 경우 영향평가의 독립성을 심각하게 저해 할 수 있으므로, 구축사업과 분리하여 별도의 사업으로 발주 필요

- 다만 불가피하게 시스템 구축 사업의 일부로 발주하거나 개인정보보호컨설팅 사업의 일부로 발주하는 경우, 영향평가 사업비용은 별도 분리해야 하며 독립성이 훼손되지 않도록 사업 추진 필요
- 정보시스템 구축사업을 감리한 업체가 동일한 사업에 대한 영향평가 수행은 불가
- 정보시스템 구축사업을 수행한 사업자가 동일한 사업에 대해서 영향평가 사업을 수행하는 것은 불가

● 대상기관은 제안서 평가 시 투입인력의 인증서 보유 여부 확인 필요

- 영향평가 사업은 인증서 보유 등 자격요건을 갖춘 인력만 수행 가능
- 투입인력은 평가기관에 소속되지 않더라도 전체 인력의 50% 미만에 한해 인증서를 보유한 프리랜서나 타사 인력 활용 가능

※ 인증서 보유여부는 개인정보보호 포털(privacy.go.kr) 영향평가 수행인력 조회메뉴에서 인증번호를 사용하여 조회가능

2.2. 영향평가 기관 선정

- 영향평가기관 중 제안요청사항을 충족할 수 있는 적정 기관을 선정하되, 다음과 같은 문제점이 있으면 평가 수행 업체로 부적절하므로 선정시 유의
  - 영 제37조(평가기관의 지정 및 지정취소)제5항 및 영향평가 고시 제8조(사후관리)에 따라 보호위원회로부터 개선권고, 경고, 지정취소 등을 받은 경우

제2절 영향평가 수행단계

1. 영향평가 수행계획 수립

목 표	효율적인 평가 수행을 위해 사전 계획 수립
개 요	사업 주관 부서가 영향평가 수행계획을 수립하고, 수립한 계획서는 착수회의를 통하여 영향평가팀은 물론 당해 사업과 관련하여 협조가 필요한 유관 부서, 외부기관, 외부 전문가 등과 공유
수행주체	영향평가 팀
참고자료	영향평가 수행계획서 작성 예시
산 출 물	영향평가 수행계획서

1.1. 영향평가 수행계획 수립

- 영향평가팀은 평가과정에 필요한 사항들을 정리하고 영향평가팀 내에서 공유할 수 있는 세부적인 영향평가 수행계획을 수립하여 "영향평가 수행계획서"를 작성
- 영향평가 수행계획서에는 다음과 같은 사항을 반영
  - 영향평가 수행계획서 내 반영 사항 : 평가목적, 평가대상 및 범위, 평가주체(영향평가팀), 평가기간, 평가절차(방법), 주요 평가사항, 평가기준 및 항목, 자료수집 및 분석계획 등
- 개인정보 보호책임자 등에 영향평가 수행계획서를 보고하고, 영향평가 대상사업 최종 책임자의 영향평가 수행 지시 후 평가를 실시
  - 영향평가의 필요성 공유 및 원활한 업무협조를 위해 당해 정보화사업과 관련된 유관부서 및 외부기관 등과 함께 착수회의를 실시

영향평가 수행계획서 작성 예시

목차	주요 내용	참고자료
1. 평가 목적	영향평가 수행 필요성 및 추진 배경 등을 기술	필요성 검토 질문서
2. 평가 대상	평가대상이 되는 정보화사업(정보시스템)명칭 기술	제안요청서(RFP), 사업계획서 등
3. 평가 주체	영향평가팀 구성 현황	영향평가팀 구성 및 운영 계획서
4. 평가 기간	영향평가 착수시점부터 완료시점까지의 평가기간을 산정하여 기술	영향평가기관 선정 단계에서 산출물 및 협의내용, 영향평가 수행안내서 참고
5. 평가 절차(방법)	영향평가 수행안내서 등을 참조하여 평가 절차 및 단계별 주요 수행사항 및 기간 등 기술	
6. 주요 평가사항	중점적으로 평가되어야 하는 사항 기술	
7. 평가기준 및 평가항목	영향평가 수행안내서에서 표준적으로 요구되는 평가항목(표)와 해당 사업의 특정 IT 기술 활용 여부 확인 ※ 부록으로 영향평가 항목 첨부	
8. 자료수집 및 분석계획	영향평가 수행 시 분석하여야 하는 관련 참고자료를 확인하여 해당 기관과 관련 있는 자료 파악	개인정보 관련 정책, 법규 검토 단계의 산출물 참조
9. 평가결과의 정리	영향평가 결과로 도출된 산출물(보고서)과 이를 활용하여 당해 사업에 적용하기 위한 방안 등 기술	영향평가팀 회의 내용 등 참조
10. 품질관리 방안	영향평가 결과의 품질 보장을 위한 상세 방안 기술	영향평가 품질검토 체크리스트 등 참고

1.2. 영향평가팀 구성방안 협의

- 평가기관의 PM(Project Manager : 프로젝트 책임자)은 대상기관 사업관리 담당자의 협조 하에 개인정보 보호 담당자, 유관부서 담당자, 외부전문가 등의 참여를 요청
  - 위탁 개발·관리되고 있는 정보시스템의 경우에는 실제 업무담당자와 사업담당자가 다르므로 현업 업무담당자는 반드시 참여
  - 공공기관이 사업을 추진하나 실제 정보화사업 운영·관리를 산하기관 등 외부기관이 주관한다면 해당 산하기관 담당자 참여
  - 외부 정보시스템 구축업체에 용역을 의뢰하여 구축사업을 추진 시, 프로젝트관리자(PM) 또는 파트리더(PL) 등이 참여

1.3 영향평가팀 역할 정의

- 영향평가팀의 평가기관 PM은 각 구성원의 역할 및 책임 사항을 배분
  - 영향평가팀원으로 참여하는 담당자의 업무를 정의하고, 사업관련 자료를 명확히 하여 업무의 중복 지양
- 다음 표는 영향평가 단계별로 영향평가팀의 역할관계를 정의한 것으로서, 이를 참조하여 역할 배분 가능
  - 영향평가팀은 대상기관 사업주관부서와 기관 내 유관부서 및 외부기관, 사업구축 부서를 기본적으로 포함
    ※ 외부용역을 통해 개발하는 경우, 정보시스템 개발업체(개발용역업체)를 포함
  - 개인정보보호를 위한 법률해석의 자문이 필요하거나 전문가의 조언이 필요한 경우, 외부 자문위원 포함 가능
- 영향평가기관의 평가수행 인력은 반드시 상주, 품질관리 담당자는 비상주 가능
  - 영향평가 업무의 연속성 확보 및 품질 제고를 위해 투입인력 중 최소 1명 이상은 업무분석 단계부터 위험분석, 개선계획 도출 등 사업 전기간 동안 상주

영향평가팀 역할 구분

구분	역 할
개인정보 보호책임자	- 영향평가 총괄
대상기관 사업주관부서	- 영향평가 사업관리 - 영향평가 사업 진행 단계별 산출물 등에 대한 품질관리·검토 - 기관 내 업무 유관부서 협력요청 - 영향평가팀 착수회의, 중간보고 및 종료회의 등 공식 회의 주관 - 개선계획 이행 관리 및 확인
영향평가기관	- 평가계획 수립 - 영향평가 팀 구성 - 영향평가 사업 수행 - 평가업무 간 수집된 자료와 산출물에 대한 보안관리, 품질관리 - 평가를 위한 중간 산출물 및 영향평가서 작성 - 영향평가 이행점검(발주기관 요청 시)
유관 부서, 외부기관	- 당해 사업 관련 자료 및 영향평가팀이 요청하는 자료의 제공 - 영향평가팀 요청에 의한 인터뷰 참여 - 개인정보 흐름분석 결과 검토 및 의견제시 - 영향평가서의 검토 및 의견 제공

구분	역 할
시스템 개발부서	- 당해 사업 관련 자료 및 영향평가팀이 요청하는 자료 제공 - 영향평가팀 요청에 의한 인터뷰 참여 - 개인정보 흐름분석 결과 검토 및 의견제시 - 영향평가서의 검토 및 의견 제공 등 - 평가결과에 대한 개선 수행 ※ 시스템개발을 직접 수행하지 않는 경우, 외부 개발업체 담당

영향평가팀 업무 배분 예시

업무 \ 담당	평가기관	대상기관 사업주관 부서	정보통신 또는 보안 담당관	시스템 개발자 또는 운영자	분야별 개인정보 보호 책임자	개인정보 보호 책임자	최고의사 결정권자	기타
영향평가 필요성 검토		●			◎	◇		
개인정보관련 정책, 법규 및 사업내용 검토	●		◎		◎			외부 용역 업체, 외부 전문가 참여 가능
개인정보 흐름 분석	●		◎	◎	◎			
개인정보 침해요인 및 위험평가	●		◎	◎	◎			
개선계획 수립	●		◎	◎	◎			
영향평가서 작성	●				◎	◇		
영향평가서 검수 및 제출		●			◎	◎	◇	
개선계획 이행 관리	◎	●	◎	◎	◎	◎	◇	

●: 업무 주관, ◎: 지원, ◇: 승인 및 의사결정

참여자별 역할비교(참고)

● 개인정보 보호책임자, 보안담당관, 정보통신보안담당관의 고유한 역할과 영향평가팀 내에서의 역할

구분	고유 역할	영향평가팀 내 역할
개인정보 보호책임자 (개인정보총괄 관리자)	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. 개인정보 처리방침의 수립·변경 및 시행 8. 개인정보 보호 관련 자료의 관리 9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기	· 영향평가 필요성 및 수행 계획의 적절성 검토 · 점검 기준에 개인정보보호 관련 유관 법률·지침 및 기관 내 규정 등이 적절히 반영되었는지 여부 검토 · 개인정보 처리방침의 내용 검토 · 사업 착수 또는 수행 시 개인정보보호 교육의 시행 · 사업완료 후 시스템 사용자에 대한 개인정보보호 교육계획 수립 · 영향평가 개선계획의 이행 관리 및 반영 여부 확인
보안담당관	1. 연도별 보안업무추진계획 수립 및 심사분석 (보안관련 주요 성과 및 실적분석) 2. 보안(인원, 시설, 문서, 자재 등) 진단 3. 보안교육에 관한 사항 4. 비밀소유 및 처리인가자 현황조사 5. 보안서약의 집행 6. 통신보안에 관한 업무(음어·약호자재) 7. 출입통제 등 자체 방호계획 수립, 시행 8. 보안업무 기획 및 조정 등 * 국가정보보안기본지침 제5조(정보보안담당관 운영)제4항	· 평가팀에 대한 보안관리 요구사항 검토 · 보안서약, 평가팀 업무 공간 보안점검, 문서보안 등 · 평가대상사업에 따라 시스템이 설치될 공간에 대한 물리적인 보안(출입통제, CCTV 등) 요건 검토
정보통신 보안담당관	1. 정보통신 보안활동 계획 수립 2. 정보통신망 신·증설 시 보안대책 수립 3. 정보통신실, 정보통신망 및 정보자료 등의 보안관리 4. 정보통신 보안업무 지도, 감독 및 교육 5. 정보통신 보안사고 조사 및 처리 6. 정보통신시스템의 보안관리 7. 정보통신 보안업무 심사분석 관장 8. 정보통신 보안관련 지침 등 제도 개선 9. 정보통신망 취약성 진단 10. 정보통신시스템의 보안관리 11. 기타 정보통신 보안관련 업무	· 대상사업에서 소요되는 정보시스템(서버, 네트워크, 보안장비 등) 및 관련 정보자산의 보안요건 검토 및 보안취약성 (사전)진단 · 응용프로그램 설계 및 개발 시 보안요구사항 검토 · 웹서버 등의 공개서버에 대한 네트워크 보안 요건 검토 · 기타 개인정보의 노출 및 유출 가능성 진단과 이에 따른 보호대책 검토

1.4 영향평가팀 운영계획 수립

- 영향평가팀 구성과 각 구성원의 역할 및 책임 사항의 정의가 완료되면 이를 문서화한 “영향평가팀 구성·운영계획서”를 작성
  - 영향평가팀 구성·운영계획서는 평가팀원이 내부적으로 공유하여 상호간의 역할과 업무를 재확인

영향평가팀 구성·운영계획서 예시

<table>
<tr><td>사업명</td><td colspan="4">문화건강 포털사이트 구축사업에 대한 영향평가</td></tr>
<tr><td>작성자</td><td colspan="4">영향평가팀</td></tr>
<tr><td rowspan="9">영향평가팀
구성</td><td>담당업무</td><td>성명</td><td>소속</td><td>인증번호[1)]</td></tr>
<tr><td>영향평가 총괄</td><td>김○○</td><td>대상기관 업무 총괄</td><td></td></tr>
<tr><td>영향평가 수행총괄</td><td>홍○○</td><td>평가기관 PM</td><td>2000-000</td></tr>
<tr><td rowspan="2">정책 및
법적요건 검토</td><td>정○○</td><td>대상기관 업무담당자</td><td></td></tr>
<tr><td>김XX</td><td>평가기관 업무담당자</td><td>2000-000</td></tr>
<tr><td rowspan="2">개인정보 흐름분석</td><td>김○○</td><td>대상기관 업무담당자</td><td></td></tr>
<tr><td>이XX</td><td>평가기관 업무담당자</td><td>2000-000</td></tr>
<tr><td rowspan="2">시스템 및
네트워크 분석</td><td>강○○</td><td>대상기관 업무담당자</td><td></td></tr>
<tr><td>박XX</td><td>평가기관 업무담당자</td><td>2000-000</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>영향평가팀</td><td colspan="4">● 담당업무의 상세업무 정의</td></tr>
<tr><td>영향평가팀</td><td colspan="4">● 평가팀 운영 원칙, 회의 주기 및 횟수 등 명시
● 평가에 필요한 자원(예산, 자료, 공간 등) 확보에 관한 내용</td></tr>
<tr><td>영향평가팀</td><td colspan="4">● 평가계획의 수립부터 영향평가서 작성까지의 일정 작성</td></tr>
</table>

1) 인증번호 : 영향평가 전문교육 이수 및 시험을 통과한 인력에게 부여되는 인증번호로서 유효한 인증번호를 발급받은 인력만이 영향평가를 수행할 수 있음

2. 평가자료 수집

목 표	대상사업 및 개인정보보호 관련 기관 내·외부 정책환경 분석을 위한 자료 수집
개 요	개인정보보호 관련 법규 및 상위기관의 지침과 해당기관 내부규정 현황을 파악하고 당해 사업을 이해하고 분석하기 위해 필요한 자료 등 취합 및 분석
수행주체	영향평가팀
참고자료	참고자료 없음
산 출 물	평가 시 고려해야 하는 개인정보보호 관련 법률·규정 목록, 사업개요서 등

- 효율적인 영향평가 수행을 위해 평가 대상 및 개인정보 정책 환경을 분석하기 위한 관련 자료 수집 필요
  - 분석 대상자료는 기관 내·외부 개인정보보호관련 규정, 정책환경을 분석하기 위한 ① 내부 정책자료, ②외부 정책자료, ③ 대상시스템 관련자료 등으로 구분

분석 자료

항목	수집 목적	수집 대상 자료
① 내부 정책 자료	● 기관 내부의 개인정보보호 체계, 규정, 조직 현황 등 분석	· 기관 내 개인정보 보호 규정 · 기관 내 정보보안 관련 규정 · 기관 내 직제표 등
	● 개인정보취급자(정보시스템 관리자, 접근자 등), 위탁업체 등에 대한 내부 규정 및 관리·교육 체계 확인	· 개인정보 관련 조직 내 업무 분장표 및 직급별 권한 · 정보시스템의 접근권한에 대한 내부 규정 · 위탁업체 관리 규정 등 · 시스템 관리자 및 정보취급자에 대한 교육계획
② 외부 정책 자료	● 개인정보보호 정책 환경 분석	· 개인정보 보호법, 관련 지침 등 · 개인정보보호 기본계획 등
	● 영향평가 대상사업의 특수성을 반영한 정책 환경 분석	· 평가대상사업 추진 근거 법률 및 개인정보 보호 관련 법령
③ 대상 시스템 관련자료	● 정보시스템을 통해 수집되는 개인정보의 양과 범위가 해당 사업 수행을 위해 적절한지 파악	· 사업 수행 계획서, 요건정의서 · 제안서, 업무기능분해도 · 업무흐름도, 화면설계서
	● 정보시스템의 외부연계 여부 검토	· 위탁 계획서, 연계 계획서 · 인터페이스 정의서 · 메뉴 구조도
	● 정보시스템의 구조와 연계된 개인정보 보호 기술 현황 파악	· 침입차단시스템 등 보안 시스템 구조도 · 인터페이스 정의서

2.1 내부 정책자료 분석

- 대상기관의 개인정보보호 관리체계 및 규정 수립·이행 여부는 중요
- 내부 정책자료는 개인정보보호 관리체계 분석을 위한 개인정보처리방침, 개인정보 보호 정책 관련 자료, 정보보안환경 분석을 위한 시스템 구조도 등이 해당

내부 정책자료(예시)

- **(조직·체계 자료)** 기관별 개인정보 보호지침, 개인정보보호 내부 관리계획, 개인정보 처리방침, 개인정보 보호업무 관련 직제표, 개인정보보호규정, 정보보안규정 등
- **(인적 통제·교육 자료)** 개인정보 관련 조직 내 업무분장표 및 직급별 업무 권한 현황, 정보 시스템의 접근권한에 대한 내부규정, 시스템 관리자 및 개인정보취급자에 대한 교육계획, 위탁업체 관리규정 등
- **(정보보안 자료)** 방화벽 등 침입차단시스템 및 백신프로그램 도입현황, 네트워크 구성도 등

2.2. 외부 정책자료 분석

- 외부 정책자료는 공통적으로 해당되는 일반 정책자료와 대상사업에 제한적으로 적용되는 특수 정책자료가 있으며 유형은 법령, 지침, 가이드라인, 훈령 등으로 다양
  - 영향평가는 규정 준수 여부와 더불어 개인정보보호 관점에서 정보시스템을 평가·분석하므로 지침이나 가이드라인 등의 권고사항을 반영하여 평가 필요
- 개인정보보호 관련 법규 준수 여부(Compliance)를 판단할 근거자료의 확보
  - 각종 개인정보보호관련 법규 등을 분석하여 대상사업 관련 외부의 개인정보보호 정책환경을 파악

    ※ 영향평가 관련 규정은 개인정보보호 포털(privacy.go.kr)에서 확인 가능

개인정보보호 관련 주요 법규

관련 법규	주요 내용
개인정보 보호법	개인정보 처리 과정상의 정보주체와 개인정보처리자의 권리·의무 등 규정 ※ 공공·민간 구분 없이 모든 개인정보처리자에게 적용함
신용정보의 이용 및 보호에 관한 법률	개인 신용정보의 취급 단계별 보호조치 및 의무사항에 관한 규정 ※ 신용정보를 취급하는 금융회사(은행, 보험, 카드 등) 에게 적용함
위치정보의 보호 및 이용 등에 관한 법률	개인위치정보 수집, 이용·제공 파기 및 정보주체의 권리 등 규정
표준 개인정보 보호지침	개인정보취급자 및 처리자가 준수하여야 하는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부사항 규정
개인정보의 안전성 확보조치 기준	개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 최소한의 기준 규정
개인정보 영향평가에 관한 고시	영향평가 수행을 위한 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준 규정
개인정보 위험도 분석 기준	개인정보 처리시스템의 보호수준을 진단하여 암호화에 상응하는 조치필요 여부를 판단할 수 있는 기준을 규정

- 기본적인 개인정보보호 규정 외에 특정 분야에만 적용되는 규정 검토가 필요하며 각 기관의 해당 업무에 관한 개인정보보호지침, 가이드라인 등도 검토 필요
  - 예를 들면 교육 분야는 「교육기본법」 및 「초중등교육법」 내의 개인정보보호 관련 규정, 「교육기관 및 교육행정기관의 개인정보보호 업무 지침」 검토 필요
  - 평가대상사업이 민원 업무인 경우 「민원사무처리에 관한 법률」 검토 필요

특정 IT 기술 관련 규정

관련 지침	주요 내용
RFID 프라이버시 보호 가이드라인	RFID 활용 시 개인정보보호 조치 사항
위치정보의 보호 및 이용 등에 관한 법률 위치정보의 관리적·기술적 보호조치 가이드라인	위치정보 수집 및 이용 시 개인정보보호 조치 사항
바이오정보 보호 가이드라인	지문, 홍채 등 생체 정보 수집·이용 시 개인정보 보호 조치 사항

2.3 대상시스템 관련 자료 분석

- 대상사업의 추진배경, 추진목표, 사업개요 및 사업에 영향을 미치는 제반 사항에 대한 검토·분석을 실시하고, 사업 내용을 이해할 수 있도록 '사업개요서'를 작성
  - 사업추진계획서, 제안요청서(RFP), 과제수행계획서, 요구사항 정의서 등 다양한 형태의 사업 설명자료를 참조
  - 기 구축된 개인정보 처리시스템은 업무매뉴얼 등으로 검토 가능하며, 사업관련 자료 분석을 위한 수집 내용은 영향평가 수행 시 활용되므로 상세히 검토
  - 대상기관의 정보화사업 및 개인정보 수집·이용이 법률에 근거하여 추진하는 경우가 많으므로, 관련 법률 근거를 조사하고 사업개요서 내에 반영

사업 설명자료(예시)

- **(사업수행자료)** 사업추진계획서, 제안요청서, 과제수행계획서, 요구사항 정의서, (기 구축 시) 업무매뉴얼 등
- **(외부연계)** 위탁계획서, 연계계획서, 인터페이스 정의서, 아키텍처 설계서 등
- **(개발 산출물)** 시스템 설계서, 요건 정의서, 업무 흐름도, 기능 정의서, ERD(Entity Relationship Diagram), DFD(Data Flow Diagram), 유스케이스 다이어그램(Use Case Diagram), 시퀀스 다이어그램(Sequence Diagram), 테이블 정의서, 화면 설계서, 메뉴 구조도, 아키텍처 설계서, 시스템 구조도 등

3. 개인정보 흐름 분석

목 표	대상사업에서 처리되는 개인정보 흐름에 대한 파악을 위해 정보시스템 내 개인정보 흐름 분석
개 요	① 개인정보 처리업무 분석 (개인정보 영향도 등급표, 개인정보 처리업무표 및 업무 흐름도 작성) ② 개인정보 처리 업무표를 기반으로 개인정보 흐름표 작성 ③ 개인정보 흐름표를 기반으로 개인정보 흐름도 작성 ④ 기관 내 네트워크 및 보안시스템 구조 등을 분석하여 정보시스템 구조도 작성
수행주체	영향평가팀
참고자료	개발관련 산출물, 해당 업무 매뉴얼
산 출 물	개인정보 영향도 등급표, 개인정보 처리업무표, 개인정보 처리업무 흐름도, 개인정보 흐름표, 개인정보 흐름도, 정보시스템 구조도

● 개인정보 흐름분석은 4단계로 진행

① 개인정보 처리업무 분석

· 영향평가 대상 업무 중에서 개인정보 처리업무를 도출하여 평가범위를 선정

· 개인정보를 처리(수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등)하는 모든 업무를 파악

② 개인정보 흐름표 작성

· 개인정보의 수집, 보유, 이용·제공, 파기에 이르는 Life-Cycle별 현황을 식별하여 개인정보 처리현황을 명확히 알 수 있도록 흐름표 작성

③ 개인정보 흐름도 작성

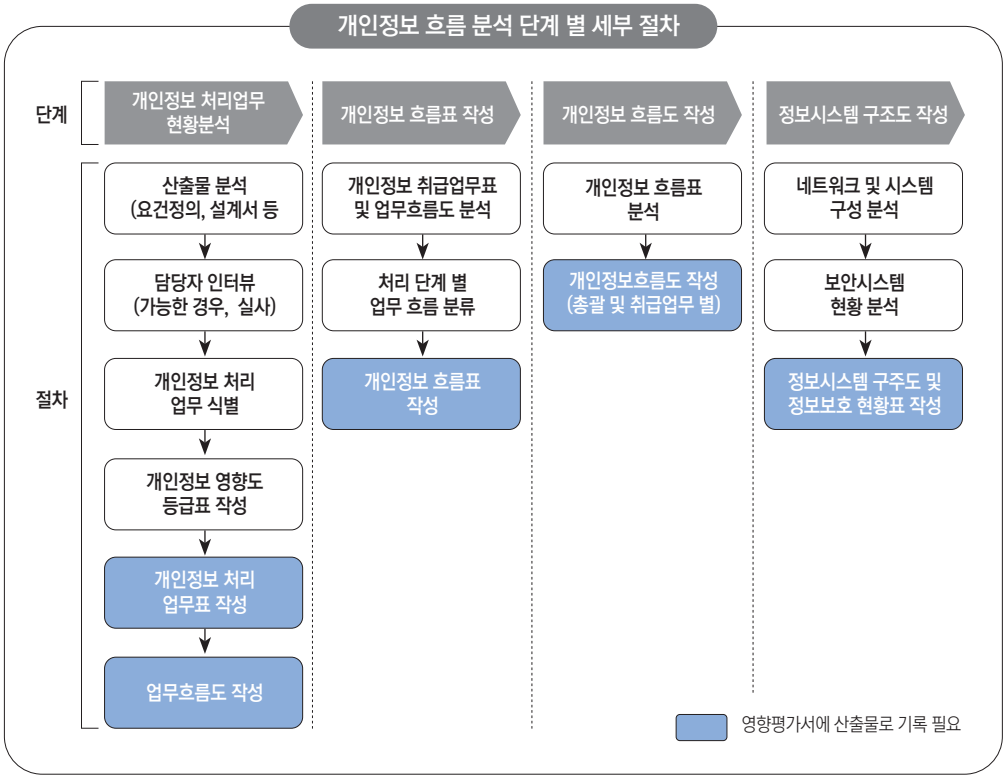
· 개인정보흐름표를 바탕으로 개인정보의 수집, 보유, 이용·제공, 파기에 이르는 Life-Cycle별 현황을 식별하여 개인정보 처리현황을 명확히 알 수 있도록 흐름도 작성

④ 정보시스템 구조도 작성

· 개인정보 처리시스템, 개인정보 내·외부 연계시스템 및 관련 인프라의 구성 파악

· 다른 단계와 병렬 진행 가능하며, 분석 초기에 작성하여 타 단계 진행 시 참고 가능

※ 흐름분석 및 개선계획 수립 단계와 관련하여 본 수행안내서에서 제시된 양식(표, 그림 등)은 예시로서, 영향평가 기관의 자체 방법론에 따라 대상 사업의 특성 등을 고려하여 양식을 추가 또는 일부 변형하여 사용할 수 있음(단 각 단계별 기본 절차는 준수하여야 하며, 영향평가 품질 측면에서 각 절차의 취지 및 목적을 달성할 수 있도록 하여야 함)



3.1 개인정보 처리업무 현황 분석

- 개인정보 처리업무 현황 분석을 위해서는 평가자료 수집 단계에서 수집한 산출물 분석을 수행하고 업무 담당자 인터뷰 및 현장 실사 등을 통해 업무이해
  - 조직도(대상기관, 개발 조직, 운영조직 등) 및 업무분장표 등을 참조하여 인터뷰 대상자를 선정하고 계획을 수립
  - 인터뷰 대상자는 시스템 개발, 운영 담당자 및 현장 업무담당자를 포함하여야 하며, 개인정보 처리 업무 분석을 위해 필요하다고 판단되는 대상자도 포함
  - 기 운영 중인 시스템의 경우에는 시스템 실사를 통해 산출물 및 인터뷰 내용의 정합성과 누락 사항 존재 여부 등에 대해 검증
  - 실사는 업무 현장 실사와 화면·DB 등에 대한 시스템 실사로 진행
- 자료분석, 인터뷰 및 현장실사를 병행하여 분석한 결과를 기반으로 개인정보 처리 업무를 식별
- 식별된 개인정보 처리업무 별로 개인정보 항목에 대한 중요도 평가를 위해 개인정보 영향도 등급표를 작성하고 등급표에 따라 영향도를 평가

특정 IT 기술 관련 규정

등급	조합설명	위험성	자산가치	분류	개인정보 종류
1등급	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	· 정보주체의 경제적/사회적 손실을 야기하거나, 사생활을 현저하게 침해 · 범죄에 직접적으로 악용 가능 · 유출 시 민/형사상 법적 책임 부여 가능 및 대외 신인도 크게 저하	5	고유식별정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 ※「개인정보 보호법」 제24조 및 동법 시행령 제19조
				민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 병력(病歷), 신체적 ·정신적 장애, 성적(性的) 취향, 유전자 검사정보, 범죄경력정보, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보 ※「개인정보 보호법」 제23조 및 동법 시행령 제18조
				인증정보	비밀번호, 바이오정보(지문, 홍채, 정맥 등) ※「개인정보의 안전성 확보조치 기준 고시」 제2조
				신용정보/금융정보	신용카드번호, 계좌번호 등 ※「신용정보의 이용 및 보호에 관한 법률」 제2조, 제1호 가목, 제1의2호, 제2호
				의료정보	건강상태, 진료기록 등 ※「의료법」 제22조,제23조 및 동법 시행규칙 제14조 등
				위치정보	개인 위치정보 등 ※「위치정보의 보호 및 이용 등에 관한 법률」 제2조, 제16조 등
				기타 중요정보	해당 사업의 특성에 따라 별도 정의
2등급	조합되면 명확히 개인의 식별이 가능한 개인정보	· 정보주체의 신분과 신상 정보에 대한 확인 또는 추정 가능 · 광범위한 분야에서 불법적인 이용 가능 · 유출시 민/형사상 법적 책임 부여 가능 및 대외 신인도 저하	3	개인식별정보	이름, 주소, 전화번호, 핸드폰번호, 이메일 주소, 생년월일, 성별 등
				개인관련정보	학력, 직업, 키, 몸무게, 혼인여부, 가족 상황, 취미 등
				기타 개인정보	해당 사업의 특성에 따라 별도 정의
3등급	개인식별정보와 조합되면 부가적인 정보를 제공하는 간접 개인정보	· 정보주체의 활동 성향 등에 대한 추정 가능 · 제한적인 분야에서 불법적인 이용 가능 · 대외 신인도 다소 저하	1	자동생성정보	IP정보, MAC주소, 사이트 방문기록, 쿠키(cookie) 등
				가공 정보	통계성 정보 등
				제한적 본인 식별 정보	회원번호, 사번, 내부용 개인식별정보 등
				기타 간접 개인정보	해당 사업의 특성에 따라 별도 정의

※ 서로 다른 등급의 개인정보가 혼재한 경우, 상위 등급의 개인정보로 선정

※ 영향도의 산정은 영향평가 기관의 고유 방법론에 따라 달라질 수 있으며 개인정보 영향도 등급표 예시에 따른 등급(1~3 등급) 또는 자산가치(5, 3, 1)의 값을 정하여 사용 가능

- 개인정보 처리업무를 구분하여 개인정보 처리 업무표를 작성
  - 업무별로 처리하는 개인정보의 누락이나 오류사항이 없도록 철저히 검토
  - 개인정보 처리 업무별 개인정보 영향도 등급표에 따라 영향도 산정

개인정보 처리 업무표 양식

평가업무명[1]	처리 목적[2]	처리 개인정보[3]	주관부서[4]	개인정보 건수[5]	개인정보 영향도[6]

개인정보 처리 업무표 양식 설명

1) 평가업무명

- 영향평가 대상시스템에서 개인정보가 처리되는 업무를 주요 업무단위로 기재
  - ※ 개인정보에 대한 관리가 가능한 범위로 유사한 업무단위로 묶어 단위업무를 구성
  - ※ 평가업무를 너무 포괄적으로 분류할 경우 평가가 부실하게 수행될 가능성이 있으므로, 중요하거나 복잡한 업무는 세분화하여 분류함으로써 평가의 구체성을 높일 필요가 있음

2) 처리 목적

- 업무에서 개인정보를 처리하는 목적 및 사유를 기재
  - ※ 개인정보처리방침이나 개인정보 수집 및 이용 동의 절차에 명시된 '개인정보의 수집·이용 목적'을 참고하여 조사 가능

3) 처리 개인정보

- 영향평가의 평가업무 단위로 처리되는 개인정보 항목 기재
  - ※ 주소, 수급자주소, 자택주소, 자택번지 등과 같이 유사한 항목이 있는 경우에도 '주소'로 대표화하지 않고, 가급적 구분하여 상세히 기재(단, 명칭만 다르고 의미가 같은 경우에는 용어를 1개로 통일하여 기재)
- 개인정보 항목 기재 시 업무처리를 위해 필수 정보인지 선택정보인지 여부를 명확히 알 수 있도록 '필수', '선택' 항목 구분 표기

4) 주관부서

- 해당 개인정보 처리 업무를 주관하는 부서명 기재
  - ※ 여러 부서가 공동으로 주관할 경우 모두 기재

5) 개인정보 건수

- 처리되는 개인정보 건수 기재
  - ※ 여러 개인정보가 혼재하여 건수가 상이한 경우, 가장 많은 정보를 기준으로 기재하며, 고유식별정보가 포함된 경우, 건수 뒤에 '( )' 후 고유식별정보의 개수를 추가 기재
  - ※ 동일한 정보주체에 대한 정보가 중복되어 존재할 경우, 중복을 제거한 건수 기재
  - ※ 신규 사업의 경우, 향후 1년 내에 예상되는 건수를 입력

6) 개인정보 영향도

● 처리 개인정보의 중요도에 따라 영향도를 산정

※ 대상사업(대상시스템)의 개인정보 처리업무, 처리되는 개인정보현황, 개인정보 항목의 조합수준에 따라 영향도를 산정하고, 자산(평가업무) 가치를 측정하여 '개인정보 영향도'를 작성

평가업무명	처리 목적	처리 개인정보	주관부서	개인정보 건수	개인정보 영향도
…	…	…	…	…	…
회원가입	본인확인	생년월일	○○사업부	10만	3
	본인확인	이메일주소	○○사업부	10만	3
	…	…	…	…	…
상담업무	본인확인	성명	○○사업부	5천	3
	본인확인	생년월일	○○사업부	5천	3
	…	…	…	…	…
실업급여 관리	사용자 인증	비밀번호	○○사업부	3만	5
	실업급여 입금	계좌번호	○○사업부	3만	5
…	…	…	…	…	…

※ 업무단위(평가업무명)별로 처리 개인정보를 그룹핑하여 하나의 셀에 정리하고 해당업무에서 처리하는 개인정보의 영향도 중 가장 높은 숫자를 입력 (아래 "개인정보 처리업무표 예시" 참고)

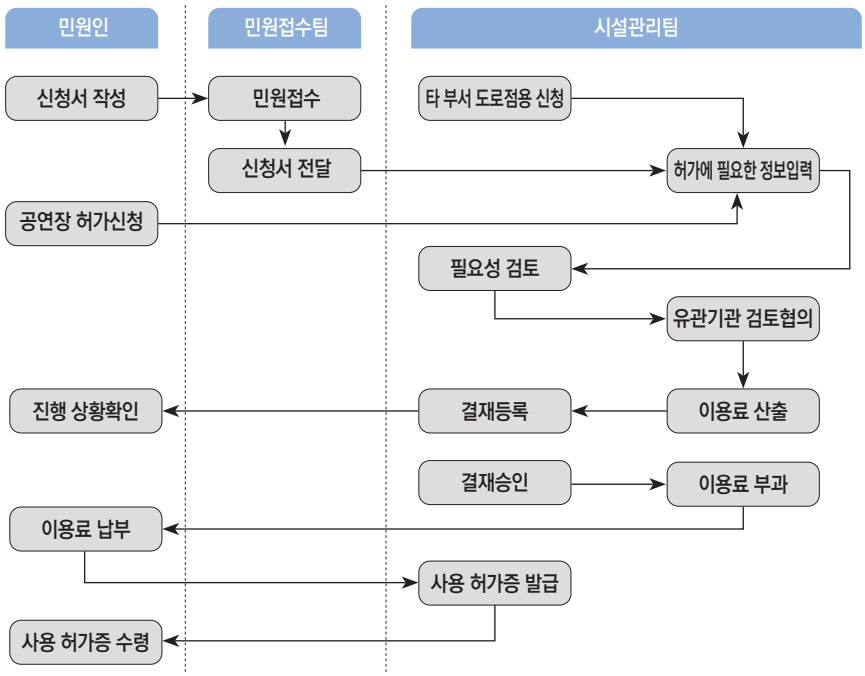
개인정보 처리 업무표 예시

평가 업무명	처리 목적	처리 개인정보	주관 부서	개인정보 건수 (고유식별정보수)	개인정보 영향도
회원관리	홈페이지 회원가입, 본인확인, 정보제공 등 회원 서비스 제공	**필수** : 성명, 생년월일, 전화번호, 이메일주소, ID, 비밀번호 **선택** : 집주소, 집전화번호	민원팀	10만건 (0건)	5
상담업무	고객 문의 및 민원 응대	**필수** : 성명, 전화번호, 상담내용	민원팀	5천건 (0건)	3
실업급여 관리	실업급여 지급확인 및 관련 절차 알림, 확인	**필수** : 성명, 주민등록번호, 계좌번호, 전화번호 **선택** : 이메일주소	민원팀	3만건 (3만건)	5
…	…	…	…	…	…

3.2 개인정보 처리 업무흐름도 작성

- 평가대상 업무현황 분석을 통해 개인정보를 처리하는 업무 별로 '업무 흐름도'를 작성
  - 정형화된 별도서식은 없으며 영향평가 기관의 서식에 맞춰 작성하고, 사업분석시 활용한 참고자료에 업무흐름도가 있으면 기존에 작성된 것을 활용 가능
  - 개인정보 처리업무 흐름도는 해당업무를 수행하는 인력 및 부서 등을 함께 표시하고, 연계기관이 있는 경우에는 해당기관도 포함하여 작성

개인정보 처리업무 흐름도(공용시설물 관리업무) 예시



3.3. 개인정보 흐름표 작성

- 분석된 업무흐름을 기반으로 개인정보 처리업무별로 개인정보의 수집, 보유, 이용·제공, 파기로 구분하여 개인정보 흐름을 분류
- 개인정보 처리 단계별로 처리되는 개인정보 현황 및 처리 내역 등을 용이하게 식별할 수 있도록 개인정보 흐름표를 작성
  - 개인정보 흐름표에는 이전 단계에서 분류한 업무명을 기준으로 개인정보의 수집, 보유, 이용·제공, 파기에 이르는 Life-Cycle별 현황을 기재하여 개인정보 흐름을 한 눈에 이해할 수 있도록 작성

개인정보 생명주기(Life-Cycle)란?

- 개인정보를 취득하여 활용하는 단계로써 통상적으로 수집, 보유, 이용·제공, 파기의 4단계로 구분
- **(수집)** 정보주체의 개인정보를 취득하는 단계로써, 통상적으로 웹사이트 회원 가입, 서면 신청서 작성, 민원 접수 등의 형태를 통해 이루어짐
- **(보유)** 수집한 개인정보를 보유하는 단계로써, 보유한 개인정보를 안전하게 관리하며 정보주체의 개인정보 열람·정정권리 등을 보장
- **(이용·제공)** 수집·저장한 개인정보를 업무적인 목적으로 이용하거나 수집한 공공기관 외의 제3의 기관에게 정보를 제공하는 행위

  ※ 예를 들어, 특정 자격제도를 운영함에 있어 자격검정시험을 주관하는 기관과 자격 제도를 운영하는 기관이 상이한 경우에는 자격검정시험 주관 기관이 합격자 명단을 자격제도 운영기관과 연계하여 제공
- **(파기)** 수집 및 이용 목적이 달성된 개인정보를 파기하는 행위를 말함

  ※ 예를 들어, 이용자가 웹사이트 회원을 탈퇴한 경우에는 특정한 사유가 없는 한 회원이 아닌 사람의 정보를 더 이상 보유하고 있을 필요가 없으므로 해당 정보를 파기해야 함

개인정보 흐름표 양식

〈수집 흐름표〉

평가 업무명[1]	수집					
	수집 항목[2]	수집 경로[3]	수집 대상[4]	수집 주기[5]	수집담당자[6]	수집 근거[7]

수집 흐름표 양식 설명

※ 수집 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

1) **평가업무명** : 대상사업 중 어떤 업무와 관련하여 개인정보를 처리하는지 기재

2) **수집항목** : 수집하는 개인정보 항목을 구체적으로 기재

3) **수집경로** : 개인정보 수집방법이 온라인 또는 오프라인 등 해당 개인정보의 취득경로 기재

※ 회원가입을 통한 수집경로는 웹사이트 회원가입, 온라인을 통한 가입, 서면신청서를 통한 오프라인 방식 등으로 구분

※ 정보주체에게 직접 수집하거나 외부기관에 의해 제공받거나 연계하는 방법으로 수집

4) **수집대상** : 개인정보를 수집하는 대상인 정보주체의 유형을 기재

※ 예를 들어, 인터넷 회원의 유형이 학생, 학부모 등으로 구분이 된다면 수집 대상도 "인터넷 회원(학생)", "인터넷 회원(학부모)"으로 나눠서 작성하여 가급적 수집하는 대상 유형을 구체적으로 기재

5) **수집주기** : 개인정보를 수집하는 주기를 기재

※ 웹사이트 회원가입의 경우, 상시적으로 수집

※ 외부기관으로부터 주기적으로 제공을 받거나, 대학 입시와 같이 특정 시기에만 수집되는 경우에는 해당 주기를 기재

6) **수집담당자** : 개인정보를 수집하는 부서 및 담당자 기재

7) **수집근거** : 수집목적에 따른 법률근거 및 사용자 동의획득 여부 기재

※ 법률에 근거한 수집일 경우 법률 조항을 구체적으로 표시

개인정보 흐름표 양식

〈보유·이용 흐름표〉

평가 업무명[1]	보유·이용							
	보유 형태[2]	암호화 항목[3]	민원 처리			통계 관리		
			이용목적[4]	개인정보 취급자[5]	이용 방법[6]	이용 목적[4]	개인정보 취급자[5]	이용 방법[6]

보유·이용 흐름표 설명

※ 보유·이용 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

1) **평가업무명** : 수집 흐름표와 동일

2) **보유 형태** : 수집한 개인정보를 보유하는 장소 및 형태를 기재

※ 수집한 개인정보는 시스템을 통해 DB에 저장하고, 신청서 등은 캐비넷 등에 보관

3) **암호화 항목** : 개인정보 저장 시 암호화하는 개인정보 항목을 기재

※ 수집한 개인정보를 DB에 저장할 때 '보유 시 암호화 항목'에 해당하고, 신청서 등 다른 매체 보유는 암호화 항목에서 제외

※ 일방향 암호화 되어 있는 경우에는 '( )' 후 일방향 암호화하였음을 표기

4) **이용 목적** : 개인정보를 이용하는 목적 기재

5) **개인정보취급자** : 수집한 개인정보를 처리하는 부서 및 사용자 기재

6) **이용 방법** : 개인정보취급자가 개인정보를 이용하는 방법 기재

※ 이용 목적 및 취급자 현황은 개인정보 이용 현황에 따라 복수로 기재

개인정보 흐름표 양식

〈제공·파기 흐름표〉

평가 업무명[1]	제공								파기			
	제공 목적[2]	제공자[3]	수신자[4]	제공 정보[5]	제공 방법[6]	제공 주기[7]	암호화 여부[8]	제공 근거[9]	보관 기간[10]	파기 담당자[11]	파기 절차[12]	분리 보관 여부[13]

제공·파기 흐름표 설명

※ 제공·파기 흐름표에서 해당 사항이 없는 경우에는 기재하지 않음

1) **평가업무명** : 수집 흐름표와 동일

2) **제공 목적** : 개인정보를 제공하는 목적을 상세히 기재

3) **제공자** : 개인정보를 제공하는 부서 및 관련 담당자 기재

4) **수신자** : 개인정보를 제공받는 타 기관, 시스템명 기재

5) **제공 정보** : 제공하는 상세 개인정보 항목을 기재

6) **제공 방법** : 개인정보 제공 시 타 기관에 제공하는 방식 및 시스템 연계 시 연계 방식 기재

7) **제공 주기** : 제공하는 개인정보 주기를 기재

8) **암호화 여부** : 정보 제공 시 제공 정보 암호화 여부 및 전송 시 암호화 여부 기재

※ 해당사항이 없는 경우에는 기재하지 않음

9) **제공 근거** : 개인정보를 제공하는 법적 근거 및 사유 기재

※ 법률에 근거한 제공일 경우 법률 조항을 구체적으로 표시

10) **보유기간** : 개인정보를 수집한 후 파기하기 전까지의 보관기간 명시

※ 보관기간은 정확한 기한이 있을 경우, 1년, 10년과 같이 표기하고, 정확한 기한이 없을 경우, '웹사이트 회원 탈퇴 시까지' 등과 같이 보유 기간 산정 원칙을 명시과 같이 보유 기간 산정 원칙을 명시

11) **파기담당자** : 개인정보를 파기하는 부서 및 담당자

12) **파기 절차** : 파기가 결정된 개인정보에 대해 파기주기와 파기방법 기재

13) **분리 보관 여부** : 법령 등에 따라 개인정보를 파기하지 않고 보관하는 경우, 보존DB 등을 구성하여 다른 개인정보와 분리 저장·관리하는지 기재 (「개인정보 보호법」 제21조제3항 참조)

개인정보 흐름표(민원처리업무) 예시

〈수집 흐름표〉

평가 업무명[1]	수집					
	수집 항목[2]	수집 경로[3]	수집 대상[4]	수집 주기[5]	수집담당자[6]	수집 근거[7]
민원 처리	**(필수)** 성명, 주민등록번호, 전화번호, 이메일 주소, 민원 내용 **(선택)** 집전화번호	온라인 (홈페이지)	민원인	상시	-	이용자 동의/ OO법제O조O항 (주민등록번호)
		오프라인 (민원신청서 작성)	민원인	상시	안내창구 담당자	이용자 동의/ OO법제O조O항 (주민등록번호)

〈보유·이용 흐름표〉

평가 업무명[1]	보유·이용							
	보유 형태[2]	암호화 항목[3]	민원 처리			통계 관리		
			이용목적[4]	개인정보 취급자[5]	이용 방법[6]	이용 목적[4]	개인정보 취급자[5]	이용 방법[6]
민원 처리	Web DB	주민등록번호, 비밀번호 (일방향)	민원 처리 및 결과 관리	민원처리 담당자, 민원 관련 업무 담당자	관리자 홈페이지의 민원처리 화면 접속	민원 현황 조회	통계 담당자	관리자 홈페이지의 통계관리 화면 접속
	민원 DB	주민등록번호, 비밀번호 (일방향)						
	캐비넷 (신청서류철)	-						

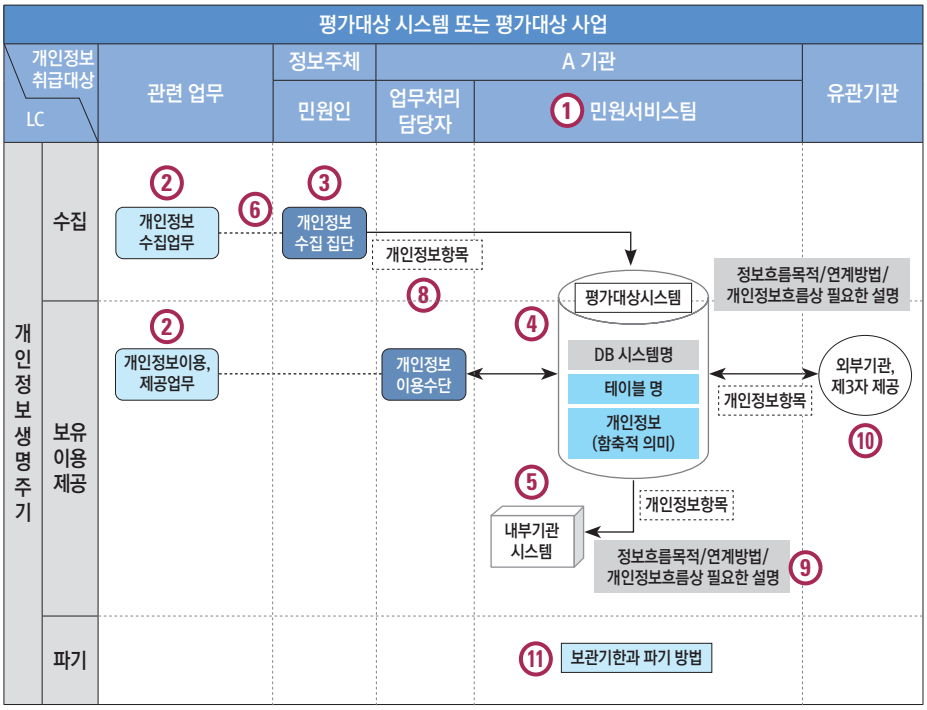
〈제공·파기 흐름표〉

평가 업무명[1]	제공								파기			
	제공 목적[2]	제공자[3]	수신자[4]	제공 정보[5]	제공 방법[6]	제공 주기[7]	암호화 여부[8]	제공 근거[9]	보관 기간[10]	파기 담당자[11]	파기 절차[12]	분리 보관 여부[13]
민원 처리	민원 처리 실적 집계	통계 담당자	OO 도청	민원인 성명, 민원 접수 내용, 처리 결과	실시간 DB 연동	상시	통신 구간 암호화 (VPN)	전자 정부법 시행령 OO조	민원 처리 완료 후 1년	DB 관리자	일단위 DB 파기	별도 보존DB 구성
									민원DB 입력 후 스캔 후 파기	통계 담당자	주단위 문서 절단	-

3.4 개인정보 흐름도 작성

- 작성된 개인정보 흐름표를 기반으로 수집, 보유, 이용·제공, 파기되는 개인정보 처리단계 별로 흐름을 한 눈에 파악할 수 있도록 '개인정보 흐름도'를 작성
- 영향평가대상사업 또는 시스템전체의 개인정보 흐름을 총괄적으로 표현한 '총괄 개인정보 흐름도'를 작성하고 개별업무별로 '업무별 개인정보 흐름도'를 함께 작성

총괄 개인정보 흐름도 범례



총괄 개인정보 흐름도 범례 설명

● 총괄 개인정보 흐름도 작성 방법

① 개인정보취급자(부서)를 정리하여 흐름도 상단에 기술

※ 취급부서 및 취급자는 필요에 따라 확장

② 개인정보 처리(수집, 보유, 이용·제공 파기)업무 기술

※ 업무에 따라 흐름도를 분리해야 할 경우, 각각 나누어 작성 가능

③ 각 업무에서 개인정보를 처리하는 수단 기술

※ 예 : PC, 신청서, 노트북, 전화, 대면, 의료기구 등

④ 개인정보를 보유하는 DB시스템을 표현하며 평가대상 시스템, DB명, 테이블명 또는 처리하는 개인정보의 함축적 의미를 가진 정보항목 기술

※ 예 : 신상정보(이름, 주민등록번호, 주소, 전화번호 등), 의료정보(혈압, 진단내용 등)

⑤ 평가대상기관 내부시스템과 연계하여 이용할 경우, 시스템명 기재

⑥ 개인정보 수집 시 수집하는 방법을 점선과 실선으로 표시

※ 온라인은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우, 점선으로 구분

⑦ 개인정보 처리과정에서 정보의 흐름방향을 화살표로 연결

⑧ 개인정보 흐름을 표시한 화살표 상에 개인정보 항목 기술

⑨ 개인정보 흐름 목적/연계방식 등 개인정보 흐름파악에 필요한 설명을 간략히 기술

⑩ 개인정보 외부제공의 경우는 외부기관명 또는 외부업체명을 기재하고 제공방식, 제공하는 개인정보 항목 기술

※ 제공방식 : 시스템 연계(VPN, EAI 등), 우편(등기), 인편, Fax, 이메일 등

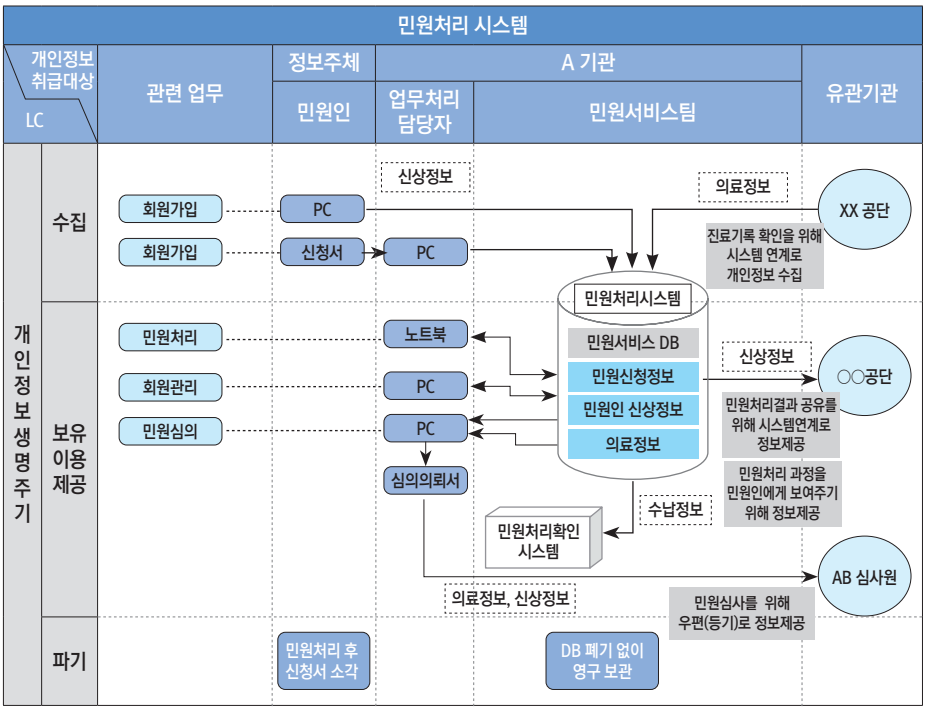
⑪ 개인정보의 보관기한과 파기 방법 기술

● 민원처리시스템에 대한 총괄 개인정보 흐름도 예시

- 개인정보 흐름도 좌측은 수집, 보유, 이용·제공 파기와 관련한 개인정보 생명주기 기입
- 개인정보 흐름도 상단은 개인정보 처리업무를 기재하고, 개인정보취급자, 담당부서, 정보주체 등 기입하며 외부기관에 제공할 경우에는 관련한 유관기관명도 기재
- 개인정보 흐름도 본문은 처리업무, 사용매체와 수집한 개인정보를 처리할 때 관련한 IT시스템을 표시하고 각 요소들 간의 이동 시 전송되는 개인정보 항목을 기재

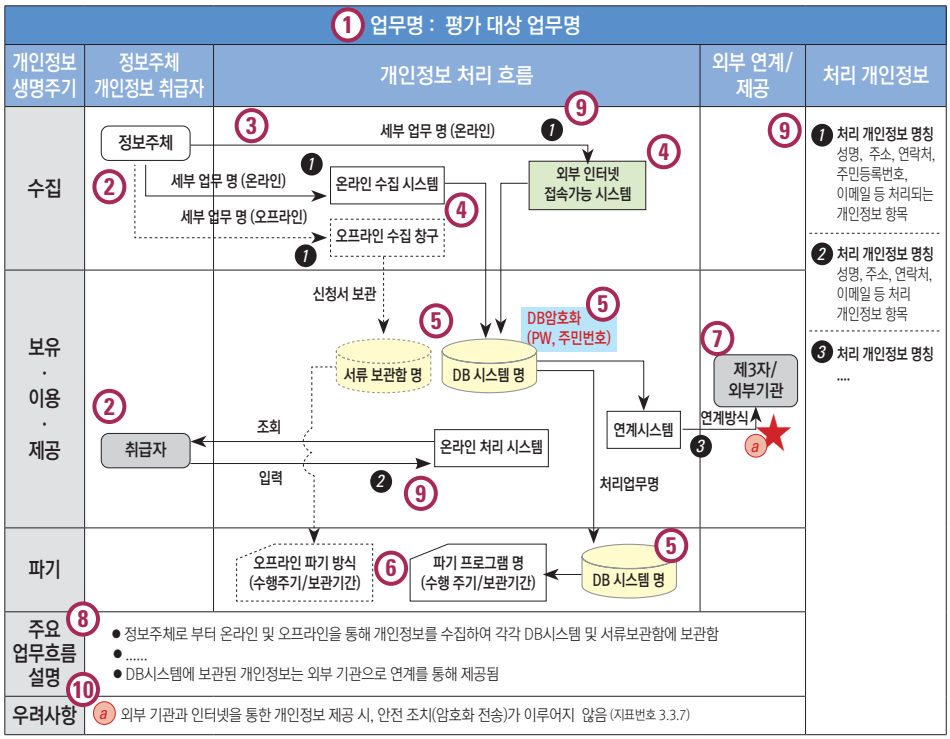
※ 총괄 개인정보 흐름도는 본 수행안내서에서 제시한 범례 및 형태를 반드시 따를 필요는 없으며, 각 영향평가기관의 방법론에 따라 다르게 표현될 수 있음

민원처리시스템 총괄 개인정보 흐름도 예시



● 업무별 개인정보 흐름도는 아래 범례를 참고하여 작성

업무별 개인정보 흐름도 범례



업무별 개인정보 흐름도 범례 설명

● 업무별 개인정보 흐름도 작성 방법

① 평가 대상 업무명을 알기 쉽게 정의하여 흐름도 상단에 기술

② 정보주체 및 취급자를 식별하여 구분하여 표시

※ 예 : 정보주체는 흰색 바탕, 취급자는 회색 바탕 도형 사용

③ 개인정보의 흐름을 간략한 세부업무 설명과 함께 점선과 실선으로 표시하고 암호화 여부를 표시

※ 온라인 흐름은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우, 점선으로 구분

※ 암호화 된 수단을 사용하는 경우, 선을 붉은 색으로 굵게 표시

④ 개인정보를 처리하는 수단을 온라인 및 오프라인으로 구분하여 표시

※ 온라인은 실선으로 하며, 오프라인으로 개인정보 흐름이 발생할 경우 점선으로 구분

※ 외부 인터넷에서 접속 가능한 시스템의 경우, 내부 시스템과 다른 색으로 구분

⑤ 개인정보를 저장하는 보관소를 대표하는 명칭으로 표기하되 DB명, 파일명 또는 서류함 등과 같이 보관 방식에 따라 적절하게 용어를 선택하여 표시

※ 캐비닛 등 오프라인 저장소의 경우 점선으로 구분

※ 암호화 보관되는 정보의 경우 암호화 항목을 박스로 별도 표시

⑥ 파기방식을 파기수행 주기와 함께 온라인 및 오프라인으로 구분하여 표시

⑦ 개인정보 외부제공의 경우는 외부기관명(또는 외부시스템) 또는 외부 업체명을 기재하고 제공방식 및 제공하는 개인정보 항목을 기술

※ 제공방식: 시스템연계(VPN, EAI 등), 우편(등기), 인편, Fax, 이메일 등

⑧ 평가대상 업무에 대한 흐름을 간략하게 설명하여 서술

⑨ 개인정보 흐름 상 전달되는 개인정보 항목을 숫자로 구분하여 도표에 표시하고 흐름도 우측에 전달되는 세부 개인정보 항목을 표시

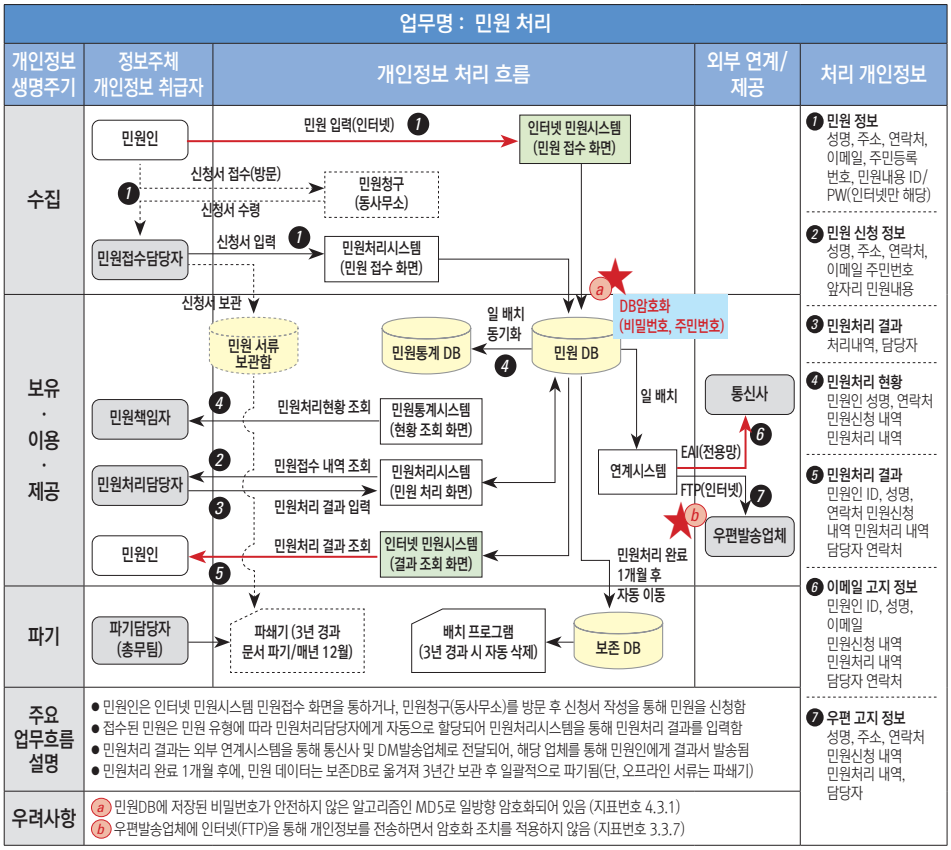
⑩ 개인정보 흐름을 통해 나타난 주요 문제점 및 관련 지표번호를 요약하여 기술

● 민원처리 업무에 대한 개인정보 흐름도 예시

- 개인정보 흐름도 좌측에 수집, 보유, 이용·제공, 파기와 관련한 개인정보 생명주기를 기입
- 개인정보 흐름도 우측에 처리 개인정보를 기재하고 개인정보 흐름에서 처리되는 개인정보 항목을 명확히 기입
- 개인정보 흐름도 상단에는 업무명를 기재하고, 개인정보처리자 및 담당부서, 정보주체 등을 기입하며 외부연계나 제공이 발생할 경우 관련기관명도 기재
- 개인정보 흐름도 하단에는 주요 업무흐름설명 및 우려사항을 기재하고, 개인정보 흐름도에 대한 간략 설명 및 예상되는 문제점을 기입
- 흐름분석 단계와 침해요인 분석단계와의 연결성 및 추적성을 확보하기 위하여 해당 우려사항과 관련된 영향평가 지표번호를 함께 기록

※ 업무별 개인정보 흐름도는 본 수행안내서에서 제시한 범례 및 형태를 반드시 따를 필요는 없으며, 각 영향평가기관의 방법론에 따라 다르게 표현 가능

민원처리 업무 개인정보 흐름도 예시



※ 각각의 평가대상 업무별로 별도의 상세 개인정보 흐름도가 작성되어야 함

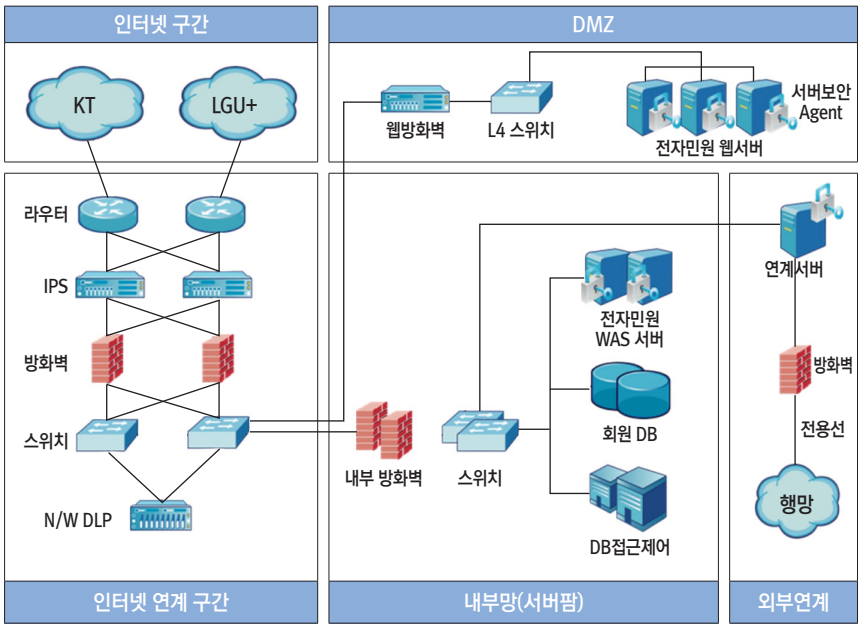
3.5 정보시스템 구조도 및 정보보호 시스템 목록 작성

- 개인정보 처리시스템과 내·외부 연계시스템 등 인프라의 구성을 파악
  - 시스템 구조, 외부 연계 및 방화벽, 침입탐지시스템 및 전송데이터 암호화, DB 암호화 등 기술적·물리적 보안시스템 현황을 분석 가능하도록 상세히 작성
  - 인터넷 구간, DMZ 구간, 외부 연계 구간, 내부망 영역 등 네트워크 성격에 따른 구분이 표시

    ※ 네트워크 접근제어의 미흡, 서비스 거부 공격에 대한 방어, 네트워크 가용성 확보 미흡 등과 같이 시스템 설계상 내재된 개인정보 침해요인을 분석, 위험도 산정 등에 활용
  - 시스템의 물리적 위치(자체 전산실, 통합전산센터 등), 관리 범위 등 영향평가 대상 시스템의 물리적·구조적 범위가 명확히 구분되도록 표시하고, 특히 서버, 데이터베이스 등 인프라 영역이 영향평가 대상 범위인지 분석하여 기록 필요
  - 정보시스템 구조도 및 정보보호 시스템 목록은 보안이 중요하여 공개가 어렵다고 판단할 경우에는 비공개로 처리 가능

    ※ 단, 비공개로 처리하더라도 시스템 구조 및 정보보호 현황 분석은 충실히 수행되어야 하며, 시스템 구조도 전체를 비공개로 처리하기 보다는 보안상 민감한 영역을 제외하거나 단순화하여 작성 필요

정보시스템 구조도 예시



- 개인정보 처리시스템에 대한 보호 대책의 적정성을 검토하고 효과적인 침해 요인 분석 및 위험도 산정이 가능하도록 '정보보호 시스템 목록'을 작성
  - 목적 및 용도, 시스템의 유형, 적용 솔루션명, 적용 대상 등에 대하여 기재
  - 해당 정보보호 시스템이 적용된 대상 구간과 시스템의 사용자가 특정인으로 한정되는 경우 사용자 등을 기재
  - 시스템이 영향평가사업 이전에 신규로 도입·적용되는 것인지, 기존에 운영 중인 정보보호 시스템이 확장 또는 변경되는 것인지 등에 대해서도 기재

정보보호 시스템 목록 예시

유형	적용 솔루션명	목적 및 용도	적용 대상	본 사업 범위 여부
방화벽	SuhoGod FW v4.0	- 인터넷과 내부 네트워크 분리 - DMZ 구성 및 접근통제 - 내부서버에 대한 접근 통제	- 인터넷 관문(이중화) - 내부 서버팜 앞단 (1)	기 운영 중
IPS	SafeZ IPS v3.5	- 인터넷에서의 네트워크 공격 탐지 및 차단	- 인터넷 관문(이중화)	기 운영 중
서버보안	SecuOS for UNIX	- 서버 계정관리, 접근통제, 이력 로깅	- UNIX 서버 전체 - Windows 계열서버 제외	○
DB접근 제어	DB Security v2.0	- DB 계정 관리, 접근통제, 개인정보 접속 기록 저장 등	- 홈페이지 회원DB - 상담DB - 민원서비스 DB	○
DB 암호화	DB Boan v1.0	- 고유식별정보 등 중요 개인정보에 대한 DB암호화	- 홈페이지 회원DB - 민원서비스 DB	○
보안USB	S-USB Plus	- 개인정보파일 등을 USB 저장/전달 시 자동암호화 - USB 분실 통제	- 민원부서 사용자(200명)	○

4. 개인정보 침해요인 분석

목 표	개인정보의 흐름에 따른 개인정보 조치사항 및 계획 등을 파악하고 개인정보 침해 위험성 도출
개 요	① 평가기준 수립 및 개인정보보호 조치사항 파악을 위한 평가항목 작성 ② 자료 분석, 현장 및 시스템 실사, 담당자 인터뷰 등을 통해 개인정보보호 조치 현황 파악 ③ 파악한 조치 현황을 기반으로 개인정보 침해요인 도출 ④ 도출된 개인정보 침해요인에 대한 위험도 산정
수행주체	영향평가팀
참고자료	내부 정책자료, 외부 정책자료, 개인정보 영향도 등급표, 개인정보 처리업무표, 개인정보 흐름표, 개인정보 흐름도, 정보시스템 구조도, 정보보호시스템 현황
산 출 물	평가항목, 침해요인 목록, 위험도 산정결과, 개선방안 목록

4.1 평가항목 구성

- 개인정보 침해요인 분석을 위한 평가항목은 5개 평가영역 25개 평가분야에 대하여 총 85개의 지표로 구성
  - 단, '1. 대상기관 개인정보보호 관리체계' 평가영역은 1년 이내에 수행된 이전 영향평가를 통해 이미 평가를 수행한 경우 대상기관과의 협의를 거쳐 제외 가능

영향평가 평가영역 및 평가분야 (「개인정보 영향평가에 관한 고시」 별표4)

평가영역	평가분야	세부분야
1. 대상기관 개인정보보호 관리체계	1.1 개인정보보호조직	개인정보 보호책임자의 지정
		개인정보 보호책임자 역할수행
	1.2 개인정보보호계획	내부 관리계획 수립
		개인정보보호 연간계획 수립
	1.3 개인정보 침해대응	침해사고 신고방법 안내
		유출사고 대응
	1.4 정보주체 권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법안내
2. 대상시스템의 개인정보보호 관리체계	2.1 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독

평가영역	평가분야	세부분야
	2.2 개인정보파일 관리	개인정보파일 대장 관리
		개인정보파일 등록
	2.3 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
3. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성
		동의받는 방법의 적절성
	3.2 보유	보유기간 산정
	3.3 이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	3.4 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	3.5 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	4.2 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	4.3 개인정보의 암호화	저장 시 암호화
		전송 시 암호화
	4.4 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업

평가영역	평가분야	세부분야
	4.5 악성프로그램 방지 등	백신 설치 및 운영
		보안업데이트 적용
	4.6 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	4.7 개인정보의 파기	안전한 파기
	4.8 기타 기술적 보호조치	개발환경 통제
		개인정보처리화면 보안
		출력 시 보호조치
	4.9 개인정보처리구역보호	보호구역 지정
5. 특정IT 기술 활용 시 개인정보보호	5.1 CCTV	CCTV 설치 시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	5.2 RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	5.3 바이오정보	원본정보 보관 시 보호조치
	5.4 위치정보	개인위치정보 수집 동의
		개인위치정보 제공 시 안내사항

- 평가항목은 침해사고 사례, 법제도의 변화, 대상기관 및 대상사업의 특성 등에 따라 추가·삭제·변경 등 탄력적으로 구성하여 사용할 필요가 있으며, 특히 개인정보보호 관련 법령·고시가 개정된 경우 해당 사항에 대해서는 반드시 평가항목에 반영하여 점검하여야 함
  - **(예시1)** CCTV 관제센터에 대한 영향평가 시, '5.1 CCTV' 분야의 평가항목에 영상정보 마스킹, 영상정보 암호화 등의 영상정보 보호 조치 평가 항목 추가
  - **(예시2)** 「개인정보의 안전성 확보조치 기준」 고시가 개정된 경우, '4. 대상시스템의 기술적 보호조치' 분야의 평가항목에 개정된 고시 내용을 반영하여 평가항목을 추가 및 변경

※ 법규는 수시로 개정되므로 평가시점에 반드시 최신 법규를 확인하여 평가항목에 반영하여야 함. 또한 법규 유예기간 중이거나 입법 예고인 상태 등에 따라 법규 시행이 확정되었거나 또는 시행 가능성이 높은 경우에는 선제적으로 평가항목에 반영할 필요가 있음

- 개인정보의 안전성 확보조치 기준과 관련된 평가항목은 대상기관의 유형에 따라 필수·선택 여부가 결정되므로, 대상기관이 어떤 유형에 속하는지 분석 필요
  - 10만명 이상의 정보주체에 관한 개인정보를 보유한 공공기관은 유형3에 해당하며, 10만명 미만의 정보주체에 관한 개인정보를 보유한 공공기관은 유형2에 해당함

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 적용 유형

<table>
<tr><th>구분</th><th>1만명 미만</th><th>10만명~10만명 미만</th><th>10만명~100만명 미만</th><th>100만명 이상</th></tr>
<tr><td>공공기간</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="2">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

  - 대상기관이 어느 유형에 해당하는지에 대한 입증책임은 당해 대상기관이 부담하게 됨
  - 개인정보 보유량은 영향평가의 대상이 되는 개인정보파일만이 아니라, 대상기관이 보유한 전체 개인정보 보유량을 기준으로 산정해야 함
  - 영향평가서 내에 대상기관이 어떤 유형에 속하는지 명확히 정의한 후, 이를 근거로 평가항목 별로 필수와 선택 여부를 지정하여 평가를 수행할 필요가 있음

4.2. 개인정보 보호조치 현황파악

- 대상 사업의 특성에 맞게 작성된 평가항목을 바탕으로 자료검토, 시스템 점검, 현장실사, 인터뷰 등을 통해 개인정보보호 조치사항을 파악하여 분석

평가항목 예시

세부분야	개인정보보호 책임자의 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.1.1	● 개인정보 보호책임자를 법령 기준에 따라 지정하고 있습니까?		○		
평가 예시	● 이행 : 개인정보 보호책임자를 법령 기준에 따라 지정하고, 지침 또는 직무기술서, 임명장 등 관련 문서 등을 통해 개인정보 보호책임자의 지정사실을 알리고 있는 경우 ● 부분 이행 : 개인정보 보호책임자가 지정되어 있으나 법률기준을 만족하지 못하거나, 지정사실을 전체 직원이 알 수 있도록 공식화하지 않은 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 4급 이상의 공무원 자격 기준을 만족하고 있는 자를 개인정보 보호책임자로 지정하여야 하나, 현재 5급 공무원이 책임자로 지정되어 있음				

- 질의문 : 평가 항목에 따른 체크리스트
- 확　인 : 평가기준은 다음과 같음

평가기준	내용
이행 (Y)	**정상적으로 조치되어 있음** - 점검항목에 대해 실제 이행, 적용하고 있고 그 사실에 대한 정확한 근거(문서)가 존재하는 경우
부분이행 (P)	**부분적으로 조치되어 있음** - 점검항목에 대해 이행, 적용하고 있으나 정확한 근거(문서) 없이 인터뷰에 의하여 계획으로만 되어 있거나 이행, 적용여부의 확인이 어려운 경우
미이행 (N)	**해당사항에 대해 조치된 바 없음** - 점검항목에 대해 실제 이행, 적용하지 않고 있거나 계획도 없는 경우
해당없음 (N/A)	**해당사항 없음** - 점검항목이 대상사업과 무관한 경우

※ Y : Yes, P : Partial, N : No, N/A : Not Applicable

- 평가 근거 및 의견 : '확인' 부분에 이행, 부분이행, 미이행, 해당없음이라고 평가한 상세근거 및 사유를 기재하고, 관련 규정이 있는 경우 근거 조항 기재
- 항목 설명 : 평가항목의 추가적인 설명 및 용어 설명 제시
- 평가 예시 : 평가 질의문의 '확인'란에 해당하는 이행(Y), 부분이행(P), 미이행(N), 해당 없음 (N/A)을 판단하는 예시 제시
- 관련 법령 및 근거 : 평가 질의문에 관한 내용을 규정하는 법, 규정 등 관련 문서 제시

지표평가 시 주의사항

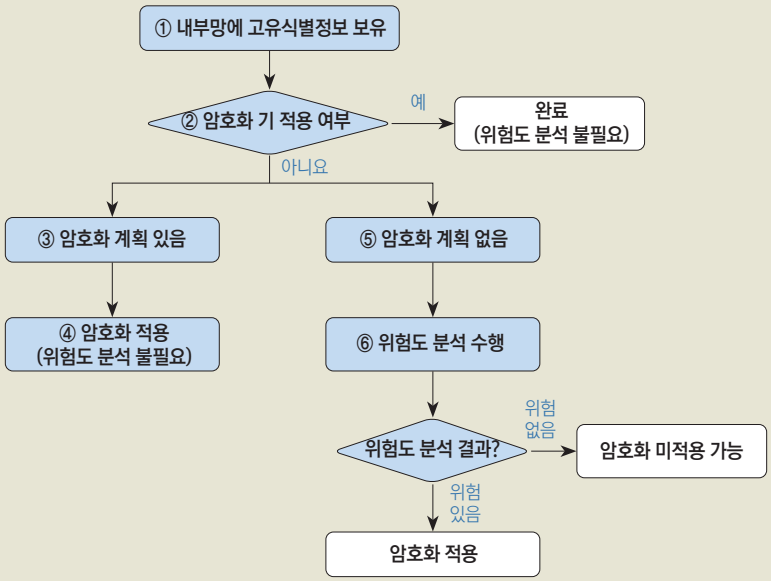
본「개인정보 영향평가 수행안내서」부록3 "개인정보 영향평가 항목(평가표)"을 참고하여 평가를 수행하되, 대상 기관 및 대상 시스템의 특성과 평가시점에서의 최신 IT기술 및 보안위협 동향, 법 규정 변경 사항 등을 반영하여 평가를 수행하여야 한다. 특히,「개인정보 보호법」등 관련 법 규정은 수시로 개정되는 경우가 많으므로 반드시 최신 법령을 기반으로 평가가 수행될 수 있도록 하여야 한다.

- 고유식별정보(주민등록번호 제외)가 내부망에 저장될 때에는 영향평가 또는 위험도분석 결과에 따라 암호화 여부의 결정이 가능
  - 고유식별정보 암호화 적용 계획이 있거나 적용되었다면 위험도 분석 불필요
  - 주민등록번호는 법제24조의2제2항에 따라 위험도 분석 결과에 상관없이 저장시 암호화 필요

※「개인정보 보호법 시행령」제21조의2에 따라 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 경우 2017년1월1일 이전까지, 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 경우 2018년1월1일 이전까지 암호화 조치 적용

고유식별정보 암호화 적용여부 판단 절차

- 고유식별정보는 「개인정보 보호법」 제24조, 제29조 및 「개인정보의 안전성 확보조치 기준」 고시에 따라 암호화 적용 필요
- 단 내부망에 고유식별정보(주민등록번호 제외)를 저장하는 경우, 「위험도 분석」 결과에 따라 암호화의 적용 여부 및 적용범위를 정하여 시행 가능



① 외부망 또는 DMZ에 고유식별정보를 저장할 경우 필수적으로 암호화를 적용하여야 함. 다만 내부망에 고유식별정보를 저장할 경우 영향평가 또는 위험도 분석에 근거하여 암호화 적용 여부 및 적용범위를 결정 가능

② 내부망에 저장된 고유식별정보가 암호화 되어 있지 않을 경우 암호화 계획 수립 여부 검토

③ 암호화 계획이 수립되어 있을 경우 별도 위험도 분석 실시 불필요

④ 암호화 계획에 따라 암호화 적용

⑤ 암호화 계획이 없을 경우 위험도 분석 수행 필요하며, 영향평가에 포함하여 수행하거나 공공기관 자체적으로 수행 가능

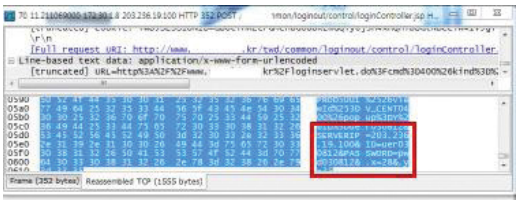
⑥ 「개인정보 위험도 분석기준」에 따라 위험도 분석 수행 후 고유식별정보에 대한 암호화 적용 여부 최종 결정

※ '개인정보 위험도 분석 기준 및 해설서' 참고

※ 단, 주민등록번호는 위험도 분석 결과와 상관없이 암호화 (시행령 제21조의2 참조)

- 개인정보 취급업무 및 개인정보 흐름이 다수 존재하는 경우에는 각 흐름별로 관련된 평가항목에 대하여 각각 평가 수행
  - 개인정보 흐름분석 결과와 침해요인 분석 결과 간의 연계성 확보 필요
- 평가항목 별 평가 결과는 상세한 근거와 함께 정리하여 기재
  - 부분이행(P), 미이행(N) 뿐 아니라 이행(Y), 해당없음(N/A)으로 평가된 항목에 대해서도 평가 결과와 근거를 상세한 사유 및 증적과 함께 제시
  - 평가 사유 및 증적은 단순히 담당자 인터뷰 결과만을 근거로 제시하는 것은 지양하며 정확한 사실에 기반하여 관련 문서명, 증거사진, 화면캡처 등을 제시

평가항목별 결과 작성 예시(1)

질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.3.3	● 고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?			○	
평가 근거 및 의견	- ○○○웹사이트에 보안서버(SSL)가 적용되어 있지 않아 인터넷 회원의 인증정보(ID/PW), 고유식별정보 등 개인정보가 인터넷 구간에 평문으로 전송되고 있음 **[회원 로그인시 전송 데이터 캡처 결과 - ID/PW 평문 노출]** 				
항목 설명	● 웹사이트에서 ID/PW와 같은 인증정보, 고유식별정보 등 중요 개인정보를 전송하는 경우, 네트워크 도청을 통한 개인정보 노출을 방지하기 위하여 인증정보를 포함한 개인정보에 대하여 암호화하여 전송하도록 함				
평가 예시	● 이행 : 웹사이트에 보안서버(SSL)를 적용하여 인증정보, 고유식별정보 등 개인정보를 암호화하여 전송함 ● 부분 이행 : 웹사이트에 보안서버(SSL)를 적용하여 개인정보를 암호화하여 전송하고 있으나, 비밀번호 변경 등 일부 화면에서 암호화 전송이 누락됨				
관련 법률 및 문서	●「개인정보의 안전성 확보조치 기준 고시」 제7조(개인정보의 암호화)				

평가항목 별 결과 작성 예시(2)

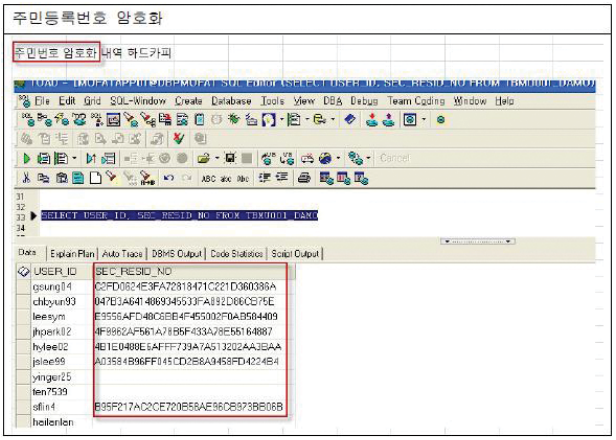
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.3.1	● 고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?	○			

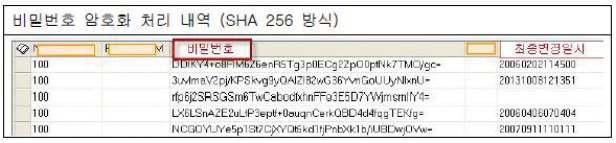
평가 근거 및 의견

– 상용 암호화 제품(○○○)을 도입하여 주민등록번호, 비밀번호에 대하여 안전한 알고리즘으로 암호화하여 저장하고 있음

▶ 주민등록번호 : 양방향 암호화(ARIA-128 알고리즘)

▶ 비밀번호 : 일방향 암호화(SHA-256 알고리즘)





항목 설명

● DB암호화는 서비스 실행에 많은 부하를 줄 수도 있으나 중요 개인정보의 경우 데이터 암호화 등의 대책을 수립하여 개인정보 유출 사고를 최대한 방지하도록 한다.

※ 고유식별정보 범위 : 주민등록번호, 여권번호, 운전면허번호 및 외국인등록번호

※ 민감정보 범위 : 사상·신념, 노동조합·정당의 가입·탈퇴에 관한 정보 등 법률에서 정한 민감정보와 유전정보 및 범죄경력에 관한 정보

평가 예시

● 이행 : 중요 개인정보가 암호화되도록 화면설계서 등의 설계문서에서 확인할 수 있는 경우

● 부분이행 : 중요 개인정보가 암호화 되도록 화면설계서 등의 설계문서에서 확인할 수 있으나 일부 개인정보에 대해서만 적용하고 있는 경우

관련 법률 및 문서

● 「개인정보 보호법」 제24조(고유식별정보의 처리 제한)

● 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)

● 「개인정보 보호법 시행령」 제21조의2(주민등록번호 암호화 적용 대상 등)

● 「개인정보의 안전성 확보조치 기준 고시」 제7조(개인정보의 암호화)

4.3 개인정보 침해요인 도출

- 개인정보 흐름 분석 및 개인정보보호 조치 현황에 대한 평가결과를 기반으로 개인정보 침해요인 분석
  - '이행(Y)' 및 '해당없음(N/A)'로 평가된 항목은 침해요인이 없는 것으로 판단
  - '미이행(N)' 및 '부분이행(P)'로 평가된 항목은 평가결과를 근거로 구체적인 침해요인 분석 및 도출 필요
- 침해요인은 유사 침해사고 사례, 대상시스템 및 업무특성 등을 반영하여 작성하고, 법률 위반 사항에 대해서는 별도로 표기 필요

침해요인 작성 예시

질의문 코드	질의문	평가근거 및 의견	개인정보 침해 요인	법적 준거성
4.3.3	● 고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?	현 시스템 및 설계서 상에 고유식별정보 등 개인정보를 홈페이지 서버로 전송 시 암호화가 적용되어 있지 않음	스니핑 등 네트워크 도청을 통해 홈페이지 회원의 고유식별정보, 인증정보가 비인가자에게 유출될 우려가 있음	개인정보 안전성 확보 조치 기준 고시 제7조 위반 (3,000만원 이하 과태료)

4.4 개인정보 위험도 산정

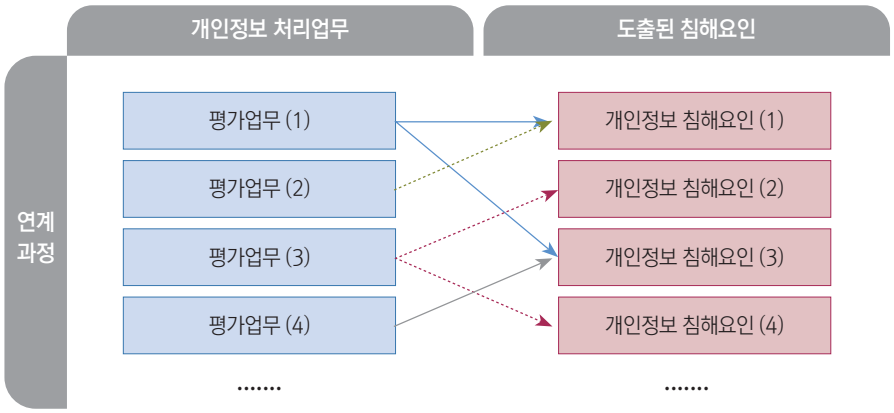
- 도출된 침해요인은 모두 개선하는 것이 원칙이나, 기관내 예산이 부족한 경우 등 불가피한 사유가 있는 경우에는 위험분석 결과에 따라 개선사항의 우선 순위를 정하여 선택적 조치 가능

  ※ 단, 법적 의무사항은 필수적으로 조치 필요
- 위험도 산정방법은 아래에서 제시된 예시 외에도 위험에 대한 관점에 따라 다양하므로, 평가기관의 자체 위험분석 방법론을 활용하여 위험도를 산정
- 다만 위험도를 산정할 때에는 아래 사항을 고려
  - 위험도 산정 과정 및 결과는 합리적이고 납득 가능한 수준이어야 함
  - 위험도 산정값은 실질적인 위험의 크기를 대변할 수 있어야 함
  - 법적 준거성 등 개인정보보호 영역의 특성이 반영되어야 함

● [위험도 산정 예시] 개인정보 영향도, 침해요인 발생가능성 및 법적 준거성에 따른 개인정보 위험도 산정 방법

- 개인정보 처리업무 내 개인정보의 조합수준, 등급 등에 따라 개인정보 처리업무의 중요도(개인정보 영향도)를 산정
- 산정된 개인정보 처리업무 영향도, 침해요인 발생가능성, 법적 준거성을 조합하여 위험도를 평가·합산하는 방법을 적용

개인정보 처리업무별 침해요인 연계 개념도



- 개인정보 처리업무의 중요도, 침해요인의 발생가능성, 법률에 규정된 의무사항 등을 종합적으로 고려하여 도출한 위험도 산정방법

개인정보 침해 위험 위험도 산정예시

위험도 = 개인정보 영향도 + (침해요인 발생가능성 × 법적 준거성) × 2

개인정보 영향도(자산 가치)

등급	설명	자산가치
1등급	- 그 자체로 개인 식별이 가능하거나 민감한 개인정보 - 관련 법령에 따라 처리가 엄격히 제한된 개인정보 - 유출 시 범죄에 직접적으로 이용 가능한 정보	5
2등급	- 조합되면 명확히 개인의 식별이 가능한 개인정보 - 유출시 법적 책임 부담 가능한 정보	3
3등급	- 개인정보와 결합하여 부가적인 정보 제공 가능 정보 - 제한적인 분야에서 불법적 이용 가능 정보	1

법적 준거성 가중치 부여

구분	법적 준거성	중요도
높음	법적 준수 사항	1.5
낮음	법률 외 요건	1

개인정보 침해요인 발생가능성

구분	발생 가능 정도	중요도
높음	즉각적인 침해 발생 가능성이 있는 경우	3
중간	침해발생 가능성이 존재하지만 즉각적이지는 않는 경우	2
낮음	침해발생 가능성이 희박한 경우	1

위험도 범위

구분	산정식	위험도
최대값	위험도 = 5 + (3 × 1.5) × 2	14
최소값	위험도 = 1 + (1 × 1) × 2	3

- 침해요인을 기반으로 관련된 개인정보 처리업무 단위로 개인정보 영향도, 침해요인 발생가능성 및 법적 준거성을 조합하여 개인정보 위험도를 산정
- 단, 위험도 산정 방식 및 가중치는 영향평가 기관의 자체 방법론 또는 대상사업의 특성 등을 고려하여 효과적인 방법을 선택하여 결정 가능 (예를 들어 법적준거성 관련 가중치값 조정, 개인정보 영향도 산정 기준으로 “개인정보파일” 단위로 변경, 위험도 산정 공식 변경 등)

개인정보 침해요인 위험도 산정 예시

개인정보 처리업무명	처리 개인정보	개인정보 영향도	질의문 코드	침해요인	발생가능성	법적 준거성	위험도
회원가입 (수집)	성명, 주민등록번호, 전화번호, 이메일 주소, 퇴직정보	5	2.2.1	변경된 부분에 대한 정보가 반영되지 않아 개인정보파일 현황을 적절히 파악하지 못해 보유하고 있는 개인정보의 관리가 어려움	3	1.5	14
회원가입 (보유·이용)	성명, 주민등록번호, 전화번호, 이메일 주소, 퇴직정보	5	3.4.1	정보주체가 위탁되는 개인정보 항목 및 위탁 목적 등을 알 수 없게 되어 정보주체의 권리를 제한할 수 있음	3	1.0	11
회원가입 (보유·이용)	성명, 주민등록번호, 전화번호, 이메일 주소, 퇴직정보	5	4.3.1	개인정보유출 사고가 발생 시 개인정보를 취득한자가 개인정보를 손쉽게 이용할 수 있음	2	1.0	9
회원가입 (파기)	성명, 주민등록번호, 전화번호, 이메일 주소, 퇴직정보	5	3.5.1	관련 법률을 위반하여 징계나 형사 벌금 등의 처벌을 받을 수 있음	3	1.5	14
민원처리 (수집)	성명, 전화번호, 주소, 이메일주소	3	2.3.2	개인정보 제3자 제공에 대한 기준이 없어 제3자에게 개인정보를 무분별하게 제공하게 될 수 있으며 정보주체의 권리가 침해될 수 있음	3	1.5	12
민원처리 (수집)	성명, 전화번호, 주소, 이메일주소	3	2.2.2	변경된 부분에 대한 정보가 반영되지 않아 개인정보파일 현황을 적절히 파악하지 못해 보유하고 있는 개인정보의 관리가 어려움	3	1.5	12
민원처리 (보유·이용)	성명, 전화번호, 주소, 이메일주소	3	2.2.1	변경된 부분에 대한 정보가 반영되지 않아 개인정보파일 현황을 적절히 파악하지 못해 보유하고 있는 개인정보의 관리가 어려움	3	1.5	12
민원처리 (보유·이용)	성명, 전화번호, 주민등록번호, 이메일주소	5	4.3.1	저장된 정보가 암호화되지 않음에 따라 개인정보유출 사고가 발생 시 개인정보를 취득한자가 개인정보를 손쉽게 이용할 수 있음	2	1.0	9
민원처리 (파기)	성명, 전화번호, 주소, 이메일주소	3	3.5.1	개인정보 미파기에 따른 법률 위반 및 과태료 처분을 받을 수 있음	3	1.5	12
...		...	...	...	...	...	

5. 개선계획 수립

목 표	개인정보 침해 요인별 위험도 분석에 기반하여, 위험요소를 제거하거나 최소화하기 위한 개선방안 및 개선계획을 수립
개 요	도출된 개인정보 침해요소에 대해 기관 내 인력 및 예산 등 자원을 고려하고 유관업무 담당자와의 협의를 거쳐 체계적으로 정비한 개선 계획을 수립함
수행주체	영향평가팀
참고자료	위험도 산정표
산 출 물	개선계획

5.1 개선방안 도출

- 식별된 침해요인별 위험도를 측정하고 검토한 후, 위험요소를 제거하거나 최소화하기 위한 개선방안 도출
  - 개선방안은 위험도의 우선순위에 따라 해당기관이 수용 가능한 수준을 정하여 단기, 중·장기로 구분하고, 수행 시기는 가능한 구체적으로 제시
  - 개선방안의 실질적인 이행을 위하여 담당부서 및 담당자를 명확히 지정

※ 법적 필수 사항은 반드시 조치될 수 있도록 개선계획 수립 필요

침해요인별 개선 방안 작성 양식 예시

위험도	개인정보 처리업무명	질의문 코드	침해요인	개선방안	수행시기	담당 부서
14	회원가입 (수집)	2.2.1	변경된 부분에 대한 정보가 반영되지 않아 개인정보파일 현황을 적절히 파악하지 못해 보유하고 있는 개인정보의 관리가 어려움	개인정보파일 변경사항을 파악하여 개인정보파일 대장에 빠짐없이 반영	2020.09 (단기)	○○ 팀
14	회원가입 (수집)	2.2.2	○○○ 개인정보파일의 보호위원회 등록이 누락됨에 따라 개인정보보호법을 위반할 수 있으며, 정보주체의 알 권리를 침해함	○○○ 개인정보파일을 내부 승인절차를 거쳐 보호위원회에 등록	2020.09 (단기)	○○ 팀
14	회원가입 (파기)	3.5.1	회원가입 서류를 관련 법률 등에 명시된 기한을 넘겨 보관하여 처벌을 받을 수 있음	법률근거 및 수집목적에 따라 보유기간으로 산정	2020.09 (단기)	○○ 팀
....	....	....	....	....		

5.2 개선계획 수립

- 도출된 개선방안을 기반으로 대상기관 내 보안조치현황, 예산, 인력, 사업 일정 등을 고려하여 개선계획 수립
- 도출된 개선계획은 위험평가 결과를 참고하여 위험도가 높은 순서의 개선방안을 먼저 실행하도록 개선계획표 작성
- 개선계획 수립 시 주요 고려사항
  - 담당자가 취약사항을 시정하기 위해 취해야 할 조치사항과 책임사항 제시
  - 위험도(시급성), 개선용이성, 예산, 인력 등을 고려하여 현실적인 일정 수립하되, 법적 의무 사항은 빠른 시일 내에 모두 개선될 수 있도록 계획 수립
  - 예산 확보 등 특별한 사유가 없는 한 개선계획은 시스템 설계·개발 시 반영하여 해당 정보화 사업 기간 내에 조치될 수 있도록 계획 수립(「개인정보 영향평가에 관한 고시」 제9조의2 및 제9조의3)
  - 대상기관에서 개선계획 이행 시 즉시 활용할 수 있도록 구체적이고 효과적인 방안 제시
  - 침해요인 별 유사 항목은 취합하여 한 개의 개선 과제로 제시 가능
  - 침해요인 도출 단계와의 연계성 및 추적성을 확보할 수 있도록 개선과제와 관련된 평가항목 번호(질의문 코드) 표기

개선 계획표 예시

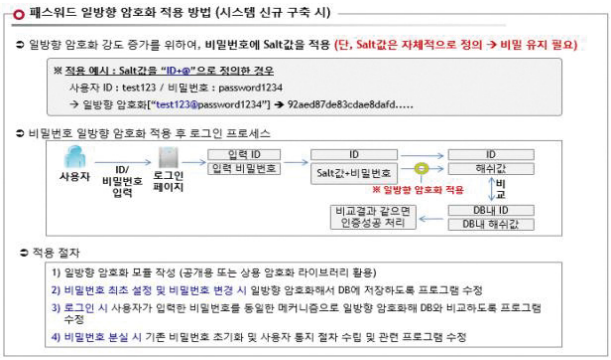
순번	개선과제명	개선내용	담당부서	수행시기
1	개인정보보호 교육 강화	- 개인정보보호 교육계획 수립(2.1.2) - 개인정보취급자에 대한 교육 수행(2.1.2)	고객보호팀	사업종료전 (2020.06)
2	개인정보 수집·저장 시 보호 조치 강화	- 회원 가입 시 입력받는 개인정보 수집항목 최소화(3.1.2) - 회원정보 DB 저장시 암호화 등의 설계 변경(4.3.1)	사업주관부서	사업종료전 (2020.06)
3	개인정보취급자 PC 보안강화	- 개인정보취급자 단말기에 키보드 해킹방지 솔루션 도입(4.8.2)	사업주관부서	2차 사업 (2021.06)
	....	....	....	....

● 도출된 개선과제에 대하여 실질적인 개선이 가능하도록 상세 개선방안 제시

- 침해요인 방지를 위한 효과적이고 구체적인 개선방안을 작성하여야 하며, 대상기관에서 과제 이행에 도움이 될 수 있도록 관련 사례가 있는 경우 함께 제시
- 평가기관의 전문성과 경험, 노하우를 활용하여 대상기관 및 시스템 관점에서 최적의 개선방안을 상세하게 제시

상세 개선방안 작성 양식 예시

<table>
<tr><td>개선과제명</td><td>1. 홈페이지 회원 비밀번호 일방향 암호화</td><td>순번</td><td>1</td></tr>
<tr><td>관련 평가항목</td><td>4.3.1</td><td>법적 요건</td><td>필수 사항</td></tr>
<tr><td>과제
상세 내용</td><td colspan="3">● 일방향 암호화 대상 정보 : 홈페이지 회원 비밀번호, 관리자 비밀번호
● 일방향 암호화 알고리즘 : SHA-256 이상 적용 필요

[보안강도에 따른 일방향(단순해쉬/전자서명용 해쉬함수) 암호 분류]
<table>
<tr><th>보안
강도</th><th>NIST(미국)</th><th>CRYPTREC(일본)</th><th>ECRYPT(유럽)</th><th>국내</th><th>안정성
유지기간(년도)</th></tr>
<tr><td>80비트
이상</td><td>SHA-1
SHA-224/256/384/512</td><td>SHA-1↑
SHA-256/384/512
RIPEMD-160</td><td>SHA-1↑
SHA-256/384/512
RIPEMD-160
Whirlpool</td><td>SHA-1↑
HAS-160
SHA-256/384/512</td><td>2010년까지</td></tr>
<tr><td>112비트
이상</td><td>SHA-224/256/384/512</td><td>SHA-256/384/512</td><td>SHA-256/384/512
Whirlpool</td><td>SHA-256/384/512</td><td>2011년부터
2030년까지
(최대 20년)</td></tr>
<tr><td>128비트
이상</td><td>SHA-256/384/512</td><td>SHA-256/384/512</td><td>SHA-256/384/512
Whirlpool</td><td>SHA-256/384/512</td><td rowspan="3">2030년 이후
(최대 30년)</td></tr>
<tr><td>192비트
이상</td><td>SHA-384/512</td><td>SHA-384/512</td><td>SHA-384/512
Whirlpool</td><td>SHA-384/512</td></tr>
<tr><td>256비트
이상</td><td>SHA-512</td><td>SHA-512</td><td>SHA-512
Whirlpool</td><td>SHA-512</td></tr>
</table>
● 비밀번호 일방향 암호화 적용 시 고려 사항 (Salt값 적용 등)
 
</td></tr>
<tr><td>담당부서
(수행 주체)</td><td>○○팀</td><td>수행 시기</td><td>2018.06</td></tr>
<tr><td>관련 법률</td><td colspan="3">-「개인정보 보호법」 제29조(안전조치의무)
-「개인정보의 안전성 확보조치 기준 고시」 제7조(개인정보의 암호화)</td></tr>
</table>

6. 영향평가서 작성

목 표	영향평가의 모든 과정 및 산출물을 정리하여 영향평가서 작성
개 요	영향평가 추진경과 및 중간산출물 등의 내용을 정리하고 도출된 위험요소 및 개선계획 등 최종 산출물들을 모두 취합하여 영향평가서를 작성하고, 대상기관은 보고서 품질을 검토함
수행주체	영향평가팀, 대상기관
참고자료	평가팀구성표, 운영계획서, 사업개요서, 평가계획서, 업무흐름도, 개인정보 흐름표, 개인정보 흐름도, 시스템구조도, 침해요인도출, 위험 평가표, 개선계획표, 영향평가항목 점검표
산 출 물	영향평가서, 품질점검 결과표

- 영향평가서는 사전 준비단계에서부터 위험관리 단계까지 모든 절차, 내용, 결과 등을 취합·정리한 문서
- 잔존 위험이나 이해관계자 간의 의견충돌이 있는 경우에는 의사결정권자(CEO, CPO 등)를 토론에 참여시켜 개인정보보호 목표수준에 대한 합의 도출
- 영향평가팀은 영향평가서를 최종적으로 검토 또는 승인할 수 있는 조직 내 최고 의사결정권자(기관장)에게 보고
- 대상기관내 다수의 개인정보처리시스템에 대하여 동시에 영향평가를 수행한 경우에는 개인정보처리시스템 단위로 영향평가서를 분리하여 작성

  ※ 단, “대상기관 개인정보보호 관리체계” 평가영역은 한 번만 작성 가능

영향평가서 작성

목차	주요 내용
표지	▶ 대상 사업명, 날짜, 사업 수행 부서 등 기재
영향평가서 개요	▶「개인정보 영향평가에 관한 고시」별지 7호 서식에 따른 개인정보 영향평가서 개요 작성
요약	▶ 영향평가에 대한 간략한 요약, 획득한 결론과 개선 사항들을 요약된 형태로 기술
목차	▶ 영향평가서의 주요 장과 절, 그리고 이들이 수록된 페이지 번호를 명시
Ⅰ. 추진 개요	
1. 사업(시스템)명	▶ 대상사업(시스템)명 기재
2. 추진 경과	▶ 평가팀 구성 등 영향평가 시작~종료시점까지 주요 경과 기술
3. 개인정보파일 개요	▶ 영향평가 대상시스템에서의 분석된 개인정보파일에 대한 내용 기술
Ⅱ. 개인정보 흐름분석	
1. 필요성 검토 결과	▶ 필요성 검토 결과 기재
2. 개인정보 처리업무표 및 업무흐름도	▶ 전체 업무 중 개인정보와 관련한 업무흐름
3. 개인정보 흐름표	▶ 개인정보 흐름표 제시 및 설명
4. 개인정보 흐름도	▶ 개인정보 흐름도 제시 및 설명
5. 시스템 구조도	▶ 대상사업의 시스템 구조도 제시
Ⅲ. 영향평가 결과	
1. 대상기관 개인정보보호 관리체계	▶ 각 분야별 조치 현황 및 침해 요인 기술
2. 대상시스템의 개인정보보호 관리체계	
3. 개인정보 처리단계별 보호조치	
4. 대상시스템의 기술적 보호조치	
5. 특정 IT기술 활용시 개인정보 보호조치	
Ⅳ. 위험평가	
1. 위험평가 개요	▶ 위험평가 개요 기술
2. 위험평가 결과	▶ 위험평가 결과 기술
3. 개선방안 도출	▶ 도출된 개선사항 정리
4. 개선계획 수립	▶ 도출된 개선사항의 이행계획 수립
Ⅴ. 총평	

● 영향평가서는 「개인정보 영향평가에 관한 고시」 별지 제7호 서식에 따라 '개인정보 영향평가서 개요'를 작성하여 영향평가서에 포함

※ 개인정보 영향평가서 개요 작성방법

<table>
<tr><th colspan="10">개인정보 영향평가서 개요</th></tr>
<tr><td colspan="2">공공기관명</td><td colspan="8">- 영향평가 대상 공공기관명</td></tr>
<tr><td rowspan="6">평가 대상 시스템 개요</td><td>시스템명</td><td colspan="2">- 영향평가 대상 개인정보처리시스템명</td><td>추진 일정</td><td colspan="4">- 대상 시스템의 사업 기간 (YYYY.MM.DD ~ YYYY.MM.DD)</td></tr>
<tr><td>추진개요 및 목적</td><td colspan="8">- 영향평가 대상 시스템 구축·변경 사업의 추진 개요 및 목적 (핵심적인 사항 중심으로 간략히 작성)</td></tr>
<tr><td rowspan="3">추진 성격</td><td>대상여부</td><td colspan="2">- 법 시행령 제35조의 각 요건 중 어디에 해당하는지 기록
①5만 이상 민감정보·고유식별정보 처리
②50만 이상 개인정보파일 연계
③100만 이상 개인정보파일 처리
④기존에 영향평가를 받은 후 변경</td><td rowspan="2">추진 예산</td><td colspan="4" rowspan="2">- 대상 시스템의 사업 비용 (단위:천원)</td></tr>
<tr><td>추진주체</td><td colspan="2">- 사업 추진 기관명</td></tr>
<tr><td>추진근거</td><td colspan="2">- 사업 추진의 근거가 되는 법령, 계획 등</td><td>비고</td><td colspan="4">- 특이사항 기록
① 신규 구축·개발
② 변경(고도화 등)
③ 표준배포시스템
④ 기타 특이사항</td></tr>
<tr><td>주요 내용</td><td colspan="8">- 사업의 주요 내용</td></tr>
<tr><td rowspan="6">개인 정보 파일 개요</td><td>개인정보 수집목적</td><td colspan="8">- 개인정보 수집목적</td></tr>
<tr><td rowspan="4">평가대상 파일</td><td colspan="2">파일명</td><td colspan="2">정보주체수</td><td colspan="4">파일 및 범위 설명</td></tr>
<tr><td colspan="2">- 영향평가 대상 개인정보파일명
※ 개인정보파일 수가 많을 경우 행을 삽입하여 추가 작성</td><td colspan="2">○○명</td><td colspan="4">- 개인정보파일에 대한 설명 기술</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="4">-</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="4">-</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="4">-</td></tr>
<tr><td>주요 개인정보 수집현황</td><td colspan="8">● 총 ( )개 항목 :
- 필수 수집 :
- 선택 수집 :</td></tr>
<tr><td rowspan="3">영향 평가 항목</td><td rowspan="3">주요 평가항목 변경 내역</td><td></td><td colspan="7">주요내용</td></tr>
<tr><td>지표추가 항목</td><td colspan="7">- 수행안내서 지표기준으로 추가된 지표 개수 및 지표번호, 지표명 기술</td></tr>
<tr><td>지표삭제 항목</td><td colspan="7">- 해당사항 없음 등의 사유로 평가에서 제외된 지표 개수 및 내용 기술</td></tr>
<tr><td rowspan="6">평가 결과 및 개선 계획</td><td rowspan="3">평가 결과 및 개선 사항</td><td>주요 내용</td><td colspan="8">● 침해요인 및 개선사항 관련 주요 내용 기술</td></tr>
<tr><td colspan="2">침해요인 도출건수</td><td colspan="2">개선대책 도출건수</td><td colspan="2">개선계획 수립건수</td><td colspan="2">조치완료 건수</td><td colspan="2">조치예정 건수</td></tr>
<tr><td colspan="2">건</td><td colspan="2">건</td><td colspan="2">건</td><td colspan="2">건</td><td colspan="2">건</td></tr>
<tr><td rowspan="2">주요개선 계획 및 일정</td><td colspan="8">● 주요 개선계획 및 일정 기술(개선계획 수가 많을 경우 행을 삽입하여 추가 작성</td></tr>
<tr><td colspan="8"></td></tr>
<tr><td>평가기관</td><td>평가기관명</td><td colspan="2">평가기간</td><td colspan="2">YYYY.MM.DD ~ YYYY.MM.DD</td><td colspan="2">평가예산</td><td colspan="2">○○천원 (VAT포함)</td></tr>
</table>

● 대상기관은 영향평가가 충실히 수행되었는지 여부에 대해 품질평가 체크리스트를 바탕으로 점검 후 미흡한 사항이 있는 경우 보완 요청

※ 개인정보 영향평가서 품질검토 체크리스트(예시)

구분	개인정보 영향평가서 개요	확인 자료
영향평가서 필수사항	1. 영향평가서는 법적 필수사항을 모두 포함하여 작성되었는가? (「개인정보 보호법」 시행령 제38조 제2항) 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	영향평가서
투입인력의 자격요건	2. 영향평가 수행 인력은 필요한 자격요건을 갖추었는가? **[투입인력 자격요건]** ※아래 3가지 요건을 모두 만족해야 함 - 자격증 : SIS(정보보안기사), 감리원, 기술사, CISSP, CISA, CPPG, 박사 - 경력 : 개인정보 영향평가 관련 분야 1년 이상 경력 - 전문교육 : 전문교육 이수 후 전문인력 인증서 획득 **[확인 방법]** - 개인정보보호 포털 → 지원마당 → 개인정보 영향평가 → 전문인력 → 전문인력 조회 (투입인력의 인증번호 및 이름으로 조회)	투입인력 인증번호
개인정보 흐름분석의 식별성	3. 평가대상 개인정보파일 및 관련 업무에 대해 총괄 개인정보흐름도 및 업무별 개인정보 흐름도가 충실히 작성되었는가? **[총괄 개인정보흐름도]** - 전체 개인정보 흐름을 한눈에 알아볼 수 있도록 작성 **[업무별 개인정보흐름도]** - 개인정보 현황분석 단계에서 분류한 개인정보 처리업무 별로 상세한 개인정보 흐름이 파악될 수 있도록 작성 - 평가대상 개인정보파일 및 개인정보 처리업무를 빠짐없이 포함하여 작성	개인정보 흐름도
	4. 개인정보흐름도는 개인정보 흐름이 명확히 식별될 수 있도록 구체적으로 작성되었는가? - 식별성을 높일 수 있도록 도형, 색상, 기호 등을 활용 - 우려사항이 있는 경우 흐름도 상에 발생위치를 표시하고 관련 평가항목 번호(지표번호)를 명시하여 평가단계별 추적성 확보 - 개인정보 수집 방법, 외부 제공 및 연계 방식, 흐름상에 전송되는 정보를 명확히 파악할 수 있도록 작성 등	

구분	개인정보 영향평가서 개요	확인 자료
평가항목의 적합성	5. 평가항목(평가지표)은 최신 법령·고시 사항이 반영되어 있는가? - 개인정보 보호법 및 시행령 - 개인정보 처리 방법에 관한 고시, 개인정보의 안전성 확보조치 기준, 표준 개인정보 보호지침 등 관련 고시 ※ 법령, 고시 개정사항은 평가항목에 즉시 반영되어야 하며, 유예기간 등시행이 확정된 사항에 대해서는 선제적 반영 필요	평가항목 (평가지표)
	6. 평가항목(평가지표)은 대상 기관 및 시스템의 특성, 최신 보안 위협 등을 반영하여 최적화 되었는가? (해당하는 경우에 한함) - 대상 기관이 특별히 적용받는 법령, 고시가 있는 경우, 관련 사항을 평가항목에 반영(의료법, 교육법 등) - 기존 평가항목에 없는 특정 IT기술을 사용하는 경우, 필요한 사항을 평가항목에 추가	
평가항목 점검의 충실성	7. 평가결과에는 오류가 없으며 평가항목별 증적이 객관적이고 상세하게 제시되었는가? - 평가증적은 제3자가 보더라도 평가결과를 납득할 수 있도록 구체적으로 제시되어야 함(화면 캡처, 설계문서 사진 등) - 법령, 고시 등 법적 요건에 대한 해석 및 점검에 오류사항이 없어야 함 - 개인정보 현황 및 흐름도, 대상 기관 및 시스템의 현황과 비교하여 점검 결과에 오류사항이 없어야 함 **[평가오류 사례]** ① 개인정보 흐름도에는 개인정보 수집 시 동의 절차가 누락된 것으로 되어 있으나, 평가항목 점검 결과에는 동의를 적절하게 받고 있는 것으로 평가 ② 개인정보 처리업무표에는 민감정보를 수집하는 것으로 표기되어 있으나, 민감정보 수집 관련 평가항목에서는 해당사항 없음으로 표기	평가항목 점검표
	8. 평가항목 점검 결과는 개인정보 흐름분석 단계와 연계성이 확보되었는가? - 개인정보 흐름분석 단계에서 식별된 개인정보 수집, 저장, 이용, 제공 및 파기 경로, 외부 위탁 관련 사항이 빠짐없이 점검되어야 함 **[평가미흡 사례]** ① 개인정보 흐름도에서는 개인정보 수집경로가 온라인(홈페이지) 및 오프라인(민원센터)이 존재하는 것으로 기록되어 있으나, 개인정보 수집 적정성 관련 평가항목 점검시 온라인 영역에 대해서만 점검하고 오프라인 영역은 점검하지 않은 경우 ② 개인정보 흐름도에서는 개인정보를 제공받는 자가 3개 외부기관으로 식별되어 있으나, 개인정보 제3자 제공 관련 평가항목 점검 시 1개 외부기관에 대해서만 점검 결과가 기록된 경우 ※관련 평가표 사례는 아래 [참고1]과 [참고2] 참고	

구분	개인정보 영향평가서 개요	확인 자료
	9. 평가항목 별로 반드시 점검해야 할 세부점검 사항이 빠짐없이 점검되었는가? - 평가항목 별로 반드시 점검되어야 할 세부 점검사항에 대해서는 빠짐없이 점검을 수행하고 점검표에 평가결과를 기록해야 함 [평가미흡 사례] ① 내부 관리계획의 적절성을 점검하면서 내부 관리계획에 반드시 포함되어야 할 항목(유형3 기준으로 15개 항목)이 모두 포함되어 있는지 여부를 확인하지 않은 경우 ② 개인정보 저장시 암호화 항목을 점검하면서 암호화 저장여부만 점검하고 안전한 암호알고리즘 사용여부를 점검하지 않은 경우 ※관련 평가표 사례는 아래 [참고3] 참고	
	10. 기술적 보호조치 관련 영역 점검 시 응용시스템 뿐만 아니라, 평가 범위에 포함된 서버, DBMS 등 인프라 영역에 대한 점검도 수행되었는가? (서버, DBMS 등 인프라 영역이 영향평가 범위에 포함된 경우에 한함) - 영향평가 범위에 서버, DBMS 등 인프라 영역이 포함되어 있는지 확인 후, 평가범위에 포함되어 있다면 평가항목별 점검 시 응용시스템 외에 서버, DBMS 영역에 대한 점검도 함께 수행 필요 ※ 계정관리(4.1.1), 인증관리(4.1.2, 4.1.4, 4.1.5, 4.1.6, 4.1.7), 권한관리(4.1.8, 4.1.9, 4.1.10), 접근통제(4.2.1, 4.2.2, 4.2.3), 인터넷 홈페이지 보호조치(4.2.5), 저장 시 암호화(4.3.1, 4.3.2), 접속기록 보관(4.4.1), 백신 설치 및 운영(4.5.1), 보안업데이트 적용(4.5.2) 등 ※ 단, 영향평가 사업의 범위, 시스템 구성, 운영형태에 따라 상이 - 표준배포시스템의 경우 중앙에서 수행한 평가지표에 대해서는 제외 가능하지만 서버, DBMS 등을 지자체에서 직접 관리하고 있다면 해당 영역에 대해서는 평가 수행 필요 **[평가누락 사례]** ① 평가 범위에 개인정보처리시스템이 운용되는 서버가 포함되어 있으나, 보안업데이트 영역 점검 시 개인정보취급자 PC에 대한 점검만 수행하고 서버OS, 웹서버(Apache, OpenSSL) 등에 대한 점검은 수행되지 않음 ② 접속기록 영역을 점검하면서 응용프로그램을 통한 접속 시 접속기록을 남기는지에 대해서는 점검을 수행하였으나, DBA 등 운영자가 DB에 직접 접속하는 경우에도 접속기록이 남는지 여부에 대해서는 점검하지 않음	
위험분석의 합리성	11. 침해요인의 내용 및 위험도의 크기는 실질적인 위험을 대변할 수 있도록 합리적으로 도출되었는가? - 침해요인의 내용은 대상 기관 및 시스템의 관점에서 어떤 문제가 있는지 명확히 알 수 있도록 구체적이고 알기 쉽게 표현되어야 함 - 법규 위반 관련 침해요인은 어떤 조항을 위반한 것이며 그로 인해 어떤 처벌과 문제가 발생할 수 있는지를 알 수 있도록 기술되어야 함 - 위험분석 절차는 논리적이고 합리적인 방법론으로 수행되어야 하며, 위험도의 크기는 대상 기관 및 시스템의 관점에서 실질적인 위험의 크기를 대변할 수 있어야 함	위험분석 결과

구분	개인정보 영향평가서 개요	확인 자료
개선 계획의 활용성	12. 침해요인 별로 개선방안이 빠짐없이 제시되었으며, 개선계획은 즉시 활용가능 하도록 구체적이고 실질적인 내용으로 수립되었는가? 도출된 모든 침해요인을 해결할 수 있도록 개선 방안이 빠짐없이 제시되어야 함 (단, 개선과제는 유사한 과제를 묶어서 제시 가능) - 각 개선방안은 해당 침해요인을 효과적으로 해결할 수 있는 최적의 방안이 제시되어야 함 - 평가기관의 일방적 제안은 지양하고, 개선방안 및 개선계획 수립시 실제 이행을 담당할 조직 및 담당자와 충분한 협의를 수행해야 함 - 개선방안 및 개선계획은 대상기관이 즉시 활용하여 이행할 수 있도록 전문적이고 상세하게 제시되어야 함 ◉ 대상 기관 및 시스템의 특성을 반영(단순 Copy & Paste 지양) ◉ 이행 관점에서 실질적인 도움이 될 수 있도록 유사 사례 제시 ◉ 평가기관의 전문성을 발휘하여 How-to 관점에서 상세 방안 제시	개선계획, 상세 개선방안

[참고1] 평가항목 점검표 사례(흐름분석 단계와 연계성)

→ 개인정보 흐름분석 단계에서 식별된 4개 개인정보파일과 6개 개인정보 수집 관련 업무에 대해 빠짐없이 점검

<table>
<tr><th>세부분야</th><th colspan="5">개인정보 수집의 적합성</th></tr>
<tr><th>질의문 코드</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>3.1.1</td><td>● 개인정보를 수집하는 경우 법령에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가 근거 및 의견</td><td colspan="5">● a1업무에서 처리하는 개인정보는 OO의 목적으로 대부분이 고등교육법, 교육기본법, 교원 자격검정령 등에 근거하여 수집되어 처리됨
● 그러나, b1업무의 채용이전에 응시원서를 통해 개인정보를 수집할 경우, 정보주체의 동의를 받고 수집하여야 하나 구체적인 동의 안내 없이 수집하고 있으며, 특히, 주민등록번호는 법률근거가 없이 수집되고 있음
● 아래 표는 평가업무별 개인정보 수집에 따른 수집 근거는 다음과 같음
<table>
<tr><th>개인정보 파일</th><th>평가업무명</th><th>수집 근거</th><th>적절성 여부</th><th>비고</th></tr>
<tr><td>A파일</td><td>- a1 업무
- a2 업무
- a3 업무</td><td>교육기본법 제 16조
고등교육법 시행령 제4조
고등교육법 시행령 제73조</td><td>○</td><td>-</td></tr>
<tr><td>B파일</td><td>- b1 업무</td><td>정보주체의 동의</td><td>×</td><td>주민등록번호 법적 수집근거 부재</td></tr>
<tr><td>C파일</td><td>- c1 업무</td><td>영유아보육법 제51조의2
영유아보육법 시행령 제26조의2
영유아보육법 시행령 제26조의3</td><td>○</td><td>-</td></tr>
<tr><td>D파일</td><td>- d1 업무</td><td>노인복지법 제39조의3
노인복지법 시행령 제26조</td><td>○</td><td>-</td></tr>
</table></td></tr>
<tr><td>증적 자료</td><td colspan="5">○○기관 개인정보 수집 증적
a1업무, a2업무, a3업무 수집 신청서 양식
b1업무 수집 신청서 양식
c1업무 수집 신청서 양식
d1업무 수집 신청서 양식</td></tr>
<tr><td>관련 법률 및 문서</td><td colspan="5">● 「개인정보 보호법」 제15조(개인정보의 수집·이용)
● 표준 개인정보 보호지침 제6조(개인정보의 수집·이용)</td></tr>
</table>

[참고2] 평가항목 점검표 사례(흐름분석 단계와 연계성)

→ 개인정보 흐름분석 단계에서 식별된 3개 수탁업체에 대해 위탁계약이 빠짐없이 체결되었는지 및 위탁계약서 내에 법적 필수 항목이 모두 포함되었는지 확인

<table>
<tr><th>세부분야</th><th colspan="5">위탁 계약</th></tr>
<tr><th>질의문 코드</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>3.4.2</td><td>● 개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가 근거 및 의견</td><td colspan="5">● ○○○시스템은 “X업체”에 시스템 유지보수 운영위탁을 위한 개인정보 위탁계약서를 작성하여 문서화하고 있으며, a1업무 운영 위탁을 위한 Y업체 개인정보처리 위탁계약서를 작성하고 있음
● 개인정보처리 위탁계약서 내에서는 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)에 따라 포함되어야 할 7가지 항목(위탁업무 수행 목적 외 개인정보의 처리금지에 관한 사항, 개인정보의 기술적 관리적 보호조치에 관한사항, 위탁업무의 목적 및 범위, 재위탁 제한에 관한 사항, 개인정보 접근제한 등 안전성확보조치에 관한 사항, 관리감독에 관한 사항, 손해배상 등 책임에 관한 사항)을 문서화하고 있음
● 그러나 b1업무를 수행하기 위한 ARS 업무 위탁을 진행하는 Z업체와는 개인정보처리 위탁계약서를 작성하지 않음
● 개인정보 위탁에 따른 수탁사 별 계약 현황은 아래와 같음
<table>
<tr><th>수탁사 명</th><th>위탁내용</th><th>위탁계약서</th><th>필수항목 포함여부</th></tr>
<tr><td>X업체</td><td>시스템 유지보수 운영위탁</td><td>○</td><td>7가지 항목 포함</td></tr>
<tr><td>Y업체</td><td>a1업무 운영위탁</td><td>○</td><td>7가지 항목 포함</td></tr>
<tr><td>Z업체</td><td>b1업무에서의 ARS 위탁</td><td>X</td><td>미포함</td></tr>
</table></td></tr>
<tr><td>증적 자료</td><td colspan="5">개인정보 처리업무 위탁계약서
X업체 위탁계약서 | Y업체 위탁계약서</td></tr>
<tr><td>관련 법률 및 문서</td><td colspan="5">● 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)
● 「개인정보 보호법 시행령」 제28조(개인정보의 처리 업무 위탁 시 조치)</td></tr>
</table>

[참고3] 평가항목 점검표 사례(세부 점검사항 점검)

→ 개인정보보호법 및 시행령에 따라 개인정보 처리방침에 반드시 포함되어야 할 11가지 사항이 모두 포함되어 있는지 확인

세부분야	개인정보 처리방침				
질의문 코드	**질의문**	**이행**	**부분이행**	**미이행**	**해당없음**
2.3.2	● 개인정보 처리방침은 법령 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?		○		

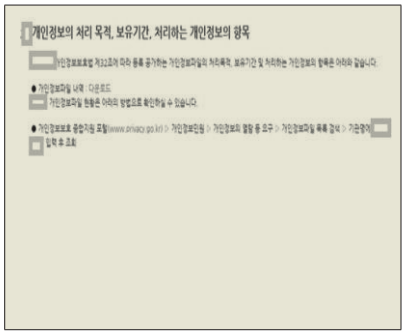
평가 근거 및 의견

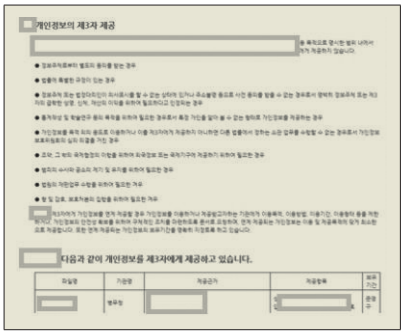
● ○○기관 홈페이지에서 안내하고 있는 개인정보 처리방침은 개인정보보호법 제30조 등에서 규정된 내용을 대부분 반영하여 수립되어 있으나, "인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치, 운영 및 그 거부에 관한 사항"이 누락됨

번호	개인정보 처리방침 기재사항	반영 여부
1	개인정보의 처리 목적	○
2	개인정보의 처리 및 보유 기간	○
3	개인정보의 제3자 제공에 관한 사항	○
4	개인정보처리의 위탁에 관한 사항	○
5	정보주체의 권리,의무 및 그 행사방법에 관한 사항	○
6	처리하는 개인정보의 항목	○
7	개인정보의 파기에 관한 사항	○
8	개인정보 보호책임자 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처	○
9	개인정보 처리방침의 변경에 관한 사항	○
10	시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항	○
11	인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치, 운영 및 그 거부에 관한 사항	X (쿠키,IP주소를 수집하고 있으나, 처리방침 미공개)

증적 자료

○○기관 개인정보 처리방침





관련 법률 및 문서

- 「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)
- 「개인정보 보호법 시행령」 제31조(개인정보 처리방침의 내용 및 공개방법 등)
- 표준 개인정보 보호지침 제19조(개인정보 처리방침의 기재사항)

- 영향평가 결과에 따른 개선사항이 사업추진 과정에서 계획대로 반영되어 개선되는지 이행점검을 통해 지속적으로 관리 필요
- 완료된 영향평가서는 해당 개인정보파일을 구축·운용하기 전에 보호위원회로 제출* (「개인정보 보호법」 시행령 제38조제2항)
  - 단, 기존에 운용 중이던 개인정보파일인 경우 영향평가 사업 완료 후 2개월 이내에 보호위원회에 제출 (「개인정보 영향평가에 관한 고시」 제12조)

    * 개인정보보호 종합지원시스템(https://intra.privacy.go.kr)에 등록

제3절 이행단계

1. 이행점검

목 표	개인정보 침해요인에 대한 조치내역을 확인
개 요	개인정보 침해요인별 조치가 필요한 사안에 대하여 그에 대한 조치결과를 확인·점검하는 과정
수행주체	사업주관부서, 평가기관 및 감리사업자
참고자료	영향평가서
산 출 물	조치내역서, 개인정보 영향평가 개선사항 이행확인서

1.1 개선사항 반영여부 점검 (개인정보파일 구축·운용 前)

- 분석·설계 단계에서 수행한 영향평가 개선계획의 반영여부를 개인정보파일 및 개인정보처리시스템 구축·운영 전에 확인
  - 대상기관은 정보시스템 분석·설계 단계에서 수행한 영향평가 결과 및 개선계획에 따라 필요한 사항을 반영
  - 감리 대상 정보화사업의 경우에는 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인
  - 감리를 수행하지 않는 경우에는 정보시스템 테스트 단계에서 자체적으로 영향평가 개선계획의 반영 여부 확인

1.2 개선사항 이행 확인

- 영향평가서를 제출받은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행 현황을 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회에 제출(「개인정보 영향평가에 관한 고시」 제14조)
  - 영향평가 시 도출된 개선계획이 예정대로 수행이 되고 있는 지 여부에 대해 점검 후 "개인정보 영향평가 개선사항 이행확인서"를 작성하여 개인정보보호위원회에 제출*

    * 개인정보보호 종합지원시스템(https://intra.privacy.go.kr)의 해당 영향평가 보고서 내 첨부
  - 개선계획 이행점검 결과는 내부 보고 절차를 거쳐 개인정보보호위원회에 제출하도록 하며, 이행점검 결과 미흡한 부분은 원인 등을 분석하여 계획대로 이행될 수 있도록 조치방안 마련
  - 단, 기존 영향평가 수행기간 내에 모든 개선사항이 조치 완료되어 개인정보보호위원회에 제출한 영향평가서에 개선과제가 없는 경우에는 '개인정보 영향평가 개선사항 이행확인서'를 제출할 필요 없음
- 개선사항에 대한 이행현황을 보호위원회에 제출할 때는 아래 양식을 활용

이행확인서 양식

◉ 개인정보 영향평가에 관한 고시 [별지 제8호서식]

개인정보 영향평가 개선사항 이행확인서					
평가영역	개선과제명	개선요구내용	이행계획 (또는 결과)	완료일 (또는 예정일)	담당자 확인

부록 1

대외유출주의

이 보고서는 ABC공공기관의 영향평가 결과자료입니다. 외부에 공개되지 않도록 유의하여 주시기 바랍니다.

ABC공공기관 홈페이지 시스템 개인정보 영향평가 결과보고서

2020년 ○○월

ABC공공기관
영향평가 사업 주관부서

개정 이력

버전	작성일	변경내용	작성자	승인자
1.0	2020.○○.○○	최초 작성	김○○	이○○

<table>
<tr><th colspan="8">영향평가서 개요</th></tr>
<tr><td colspan="2">공공기관명</td><td colspan="6">ABC공공기관</td></tr>
<tr><td rowspan="6">평가 대상 시스템 개요</td><td>시스템명</td><td colspan="2">홈페이지 시스템</td><td>추진 일정</td><td colspan="3">2020.○○.○○ ~ 2020.○○.○○</td></tr>
<tr><td>추진개요 및 목적</td><td colspan="6">홈페이지 이용자 요구사항과 운영·관리 담당자의 요구사항을 취합·반영함으로써 홈페이지에 대한 효율적 통합 운영·관리체계 확립과 이용자 중심의 서비스 품질 향상 및 신속하고 안정적인 사용자 중심의 고품질 서비스 제공</td></tr>
<tr><td rowspan="3">추진 성격</td><td>대상여부</td><td colspan="2">시스템 확대 구축</td><td rowspan="2">추진 예산</td><td colspan="3" rowspan="2">확대 구축비 : ○○원</td></tr>
<tr><td>추진주체</td><td colspan="2">ABC공공기관 시스템운영과</td></tr>
<tr><td>추진근거</td><td colspan="2">-</td><td>비고</td><td colspan="3"></td></tr>
<tr><td>주요 내용</td><td colspan="6">· 대표 홈페이지 및 관내 홈페이지, ○○○ 포털 및 통합검색 등의 통합 운영관리
· 이용자와 운영부서 의견 수렴 및 반영을 위한 수시 지원체계 운영</td></tr>
<tr><td rowspan="3">개인 정보 파일 개요</td><td>개인정보 수집목적</td><td colspan="6">○○○ 이용자 본인 확인 및 맞춤 서비스 제공</td></tr>
<tr><td rowspan="2">평가대상 파일</td><td colspan="2">파일명</td><td colspan="2">정보주체수</td><td colspan="3">파일 및 범위 설명</td></tr>
<tr><td colspan="2">ABC공공기관 통합회원 DB</td><td colspan="2">○○명</td><td colspan="3">홈페이지를 통하여 제공하는 서비스를 이용하는 통합회원 정보</td></tr>
<tr><td>주요 개인정보 수집현황</td><td colspan="6">ABC공공기관 통합회원 DB : 총 (16)개 항목
필수 수집 : 성명, 생년월일, 성별, 장애구분, ID, 비밀번호, 주소, 직업, 전화번호, 휴대폰번호, 이메일
선택 수집 : ○○○, ○○○이용목적, 관심분야, ○○○, ○○○ 성명</td></tr>
<tr><td rowspan="3">영향 평가 항목</td><td rowspan="3">주요 평가항목 변경 내역 (수행안내서 85개 지표)</td><td>구분</td><td colspan="5">주요내용</td></tr>
<tr><td>지표추가 항목</td><td colspan="5">- 개인정보보호 계획 준수 여부, 개인정보보호 계획 개정 및 이력관리 등 1개 항목</td></tr>
<tr><td>지표삭제 항목</td><td colspan="5">- RFID, 바이오 정보, 위치정보 등 활용 없어 관련 12개 항목</td></tr>
<tr><td rowspan="4">평가 결과 및 개선 계획</td><td rowspan="2">평가 결과 및 개선 사항</td><td>주요 내용</td><td colspan="6">● 결과 : ABC공공기관 홈페이지 시스템은 개인정보보호법에 의거하여 개인정보를 처리하며 개인정보보호에 필요한 내부 관리계획과 지침을 수립하고 있으나 각종 신청업무 접수 시 추가로 수집하는 개인정보에 대한 수집동의가 누락되었고, 비밀번호가 일방향 암호화하지 않으며, 개인정보파일의 보관기간이 경과한 후에도 파기하지 않는 등 일부 침해요인이 존재하므로 개선이 필요함.</td></tr>
<tr><td>개선 사항</td><td>구분</td><td>침해요인 도출건수</td><td>개선대책 도출건수</td><td>개선계획 수립건수</td><td>조치완료 건수</td><td>조치예정 건수</td></tr>
<tr><td colspan="2">주요개선 계획 및 일정</td><td colspan="6">● 2020.0월 접속기록 보관 강화
● 2020.0월 개인정보처리시스템에 대한 점검 기간 강화</td></tr>
<tr><td colspan="2">평가기관</td><td>㈜가나다 PIA기관</td><td>평가기간</td><td>2020.○○.○○ ~ 2020.○○.○</td><td>평가예산</td><td colspan="2">○○천원 (VAT포함)</td></tr>
<tr><td colspan="2"></td><td>ABC공공기관 홈페이지시스템</td><td>○○건</td><td>○○건</td><td>○○건</td><td>○○건</td><td>○○건</td></tr>
</table>

요약

ABC공공기관 홈페이지 시스템의 영향평가를 수행한 결과는 다음과 같음

"영향평가 점검표"를 기준으로 ○개 영역, ○개 평가분야, ○개 평가항목을 점검한 결과는 다음과 같음

- 양호(Y)한 항목 : ○○개 항목
- 미흡(P) 및 취약(N)한 항목 : ○개 항목
- 관련 없는 항목(NA) : ○개 항목

영향평가의 기준에 따라, ABC공공기관 홈페이지 시스템의 주요 개선사항은 다음과 같음

순번	개선과제	개선내용
1	○○, ○○, ○○ 등 신청 접수 시 추가 수집 개인정보에 대한 수집동의 획득	● 각 업무별 신청 접수 시 통합회원 가입 시 기 수집한 항목 이외에 추가로 수집하는 개인정보에 대하여 정보주체로부터 수집 동의 받을 수 있도록 개선 ● 각 업무별 신청 접수 시 추가로 수집하는 개인정보에 대하여 정보주체에게 수집사실을 알리도록 개선
2	개인정보처리업무 수탁업체에 대한 개인정보보호현황 점검 절차 수립 및 이행	● 개인정보보호규정에 개인정보 처리 위탁 시 수탁자가 준수해야 할 책임사항을 규정하고 수탁기관과의 계약서에도 해당조항을 포함하도록 개선 ● 개인정보처리업무를 위탁하는 경우 수탁자 책임사항 이행 여부 점검항목을 세분화하여 실질적인 점검이 가능하도록 보완
3	비밀번호 저장 시 일방향 암호화 알고리즘 적용	● 주요 개인정보 중 비밀번호는 관련 법령에서 정하는 바에 따라 일방향 암호화하고, 안전한 알고리즘인 SHA-256 또는 SHA-512를 적용
4	-	-

[표1] 개선계획서

목차

1. 사업의 개요 및 개인정보파일 운용의 목적	1.1 사업명	xx
	1.2 추진 경과	xx
	1.3 대상 시스템의 개요	xx
	1.4 영향평가 투입인력 및 수행비용	xx
	1.5 개인정보파일 운용의 목적	xx
2. 개인정보파일의 개요	2.1 개인정보파일의 개요	xx
3. 개인정보 흐름분석	3.1 필요성 검토 결과	xx
	3.2 평가자료 수집	xx
	3.3 업무흐름 분석	xx
	3.4 업무흐름도	xx
	3.5 개인정보 흐름표	xx
	3.6 개인정보 흐름도	xx
	3.7 네트워크 구성도	xx
	3.8 정보보호시스템 목록	xx
4. 영향평가 결과	4.1 영향평가 항목점검 결과	xx
	4.2 대상기관 개인정보보호 관리체계	xx
	4.3 대상시스템의 개인정보보호 관리체계	xx
	4.4 개인정보 처리단계별 보호조치	xx
	4.5 대상시스템의 기술적 보호조치	xx
	4.6 특정 IT기술 활용 시 개인정보보호	xx
5. 위험평가	5.1 위험평가 개요	xx
	5.2 위험도 산정 결과	xx
	5.3 개선방안 도출	xx
	5.4 개선계획 수립	xx
6. 총평	[붙임 1] 영향평가 점검항목표	xx
	[붙임 2] 개인정보 침해요인	xx

1. 사업의 개요 및 개인정보파일 운용의 목적

1.1 사업명

ABC공공기관 홈페이지 시스템 영향평가

1.2 추진 경과

ABC공공기관 홈페이지 시스템 확대 구축 및 시스템 개선 사업에 대해 영향평가를 실시하여 잠재 위험을 식별하고 침해요인 분석하여 대상시스템에 대한 개선방안을 도출하여 국민의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 최소화하는데 목적이 있음

1) 평가 기간 : 2020.○○.○○ ~ 2020.○○.○○ (약 ○개월)

2) 평가 영역

- 대상기관 개인정보 보호 관리체계
- 대상시스템의 개인정보 보호 관리체계
- 개인정보 처리단계별 보호조치
- 대상시스템의 기술적 보호조치
- 특정 IT기술 활용시 개인정보보호

3) 영향평가팀 운영계획 수립

- 영향평가 수행기관인 (주)가나다PIA기관에서 대상시스템에 대한 영향평가를 수행함
- 영향평가팀 구성

<table>
<tr><th>구분</th><th colspan="4">내 용</th></tr>
<tr><td>대상사업명</td><td colspan="4">ABC공공기관 홈페이지 시스템 확대 구축 및 시스템 개선</td></tr>
<tr><td>작성자</td><td colspan="4">영향평가팀</td></tr>
<tr><td rowspan="5">영향평가팀
구성</td><td>성명</td><td>소속/역할</td><td>담당업무</td><td>인증번호</td></tr>
<tr><td>김○○</td><td>㈜가나다
PIA기관PM</td><td>사업관리, 품질관리</td><td>2013-093</td></tr>
<tr><td>이○○</td><td>㈜가나다
PIA기관팀 수행원</td><td>주관기관 정책, 지침 및 내부 관리계획 검토
영향평가 점검항목 선정 및 검토
개인정보흐름분석 및 침해요인 실태점검 수행</td><td>2013-012</td></tr>
<tr><td>김○○</td><td>ABC공공기관
개인정보보호담당자</td><td>평가 관련 자료 수집, 제공
산출물 검토</td><td></td></tr>
<tr><td>박○○</td><td>확대구축 담당자</td><td>평가 관련 자료 수집, 제공</td><td></td></tr>
<tr><td>상세업무 정의</td><td colspan="4">영향평가팀은 대상 시스템에 대해 세부사업별로 개인정보의 수집, 보유, 제공 등의 단계에서 추가, 변경 및 삭제가 예상되는 사항을 검토하여 영향평가 결과를 보고함

[평가팀의 세부역할]
- 영향평가 총괄
· 영향평가 수행 총괄
· 필수산출물 품질 검토
· 발주기관 담당자 협의
- 영향평가 수행원
· 대상기관의 영향평가
· 대상시스템에 대한 개인정보 흐름 분석 및 영향평가 항목에 대한 점검, 평가
· 영향평가 결과보고서 등 필수산출물 작성
· 대상시스템의 침해요인 및 개선방안 도출
· 발주기관 담당자 협의
· 산출물 품질검토 및 교육</td></tr>
<tr><td>운영계획</td><td colspan="4">- 영향평가팀은 영향평가 대상시스템의 평가 시 이슈 및 검토사항에 대하여 대상기관과 협의를 위해 수시 회의 운영
- 영향평가에 대한 충분한 의견 수렴을 통해 자체 검토 항목별 개선방안 도출</td></tr>
<tr><td>추진일정</td><td colspan="4">- 전체 추진일정 2020.○○.○○ ~ 2020.○○.○○
- 사전분석
· 영향평가 필요성 검토 2020.○○.○○ ~ 2020.○○.○○
· 영향평가 계획서 작성 2020.○○.○○ ~ 2020.○○.○○
- 영향평가 실시
· 평가자료 수집 및 분석 2020.○○.○○ ~ 2020.○○.○○
· 개인정보 흐름 분석 2020.○○.○○ ~ 2020.○○.○○
· 영향평가 점검표 작성 2020.○○.○○ ~ 2020.○○.○○
· 개인정보 침해요인 도출 2020.○○.○○ ~ 2020.○○.○○
· 개선방안 도출 및 개선계획 수립 2020.○○.○○ ~ 2020.○○.○○
- 영향평가 결과정리
· 보고서 작성 2020.○○.○○ ~ 2020.○○.○○</td></tr>
</table>

[표2] 영향평가팀 운영계획 수립

4) 영향평가팀 수행계획 수립

- 평가목적
  - ABC공공기관 홈페이지 시스템 관리과정에서 개인정보의 수집·이용·연계 또는 취급 절차상 변경으로 개인의 프라이버시를 침해 및 기관의 이미지 실추, 법률 위반 등의 위험이 발생할 가능성이 있으므로 정보시스템 확대 구축 중에 개인정보 침해 위험을 사전에 방지하기 위함

- 평가 대상 및 범위
  - 평가대상 : ABC공공기관 홈페이지 시스템
  - 평가범위 : ABC공공기관 대표 홈페이지 및 통합회원관리 시스템 확대 구축사업에서 발생할 수 있는 개인정보 침해요인

- 평가 절차
  - 대상기관의 대상시스템에 대해서 행정자치부 '영향평가 수행안내서'를 기준으로 평가기관인 (주)가나다PIA 기관에서 평가하였음.

단계		수행 내용	평가방법
계획	타당성 조사	대상시스템이 수집/이용/보유하고 있는 개인정보에 대한 영향평가 필요성 여부 판단	PIA 의무대상 여부 확인 PIA 필요성 검토 질문서 확인
	평가수행 조직 구성	평가기관의 PIA의 조직구성 대상기관의 PIA의 수행조직 구성 확인	대상기관 PIA운영계획서 수행계획서 확인
	평가계획 수립	평가기관의 PIA수행 계획서 작성	
분석	평가자료 수집	대상기관의 PIA 관련 개인정보보호 법규 및 상위 기관의 지침과 내부규정 현황 검토 당해 사업이해와 분석을 위한 평가자료 검토	대상기관의 자료요청 목록 확인 담당자 인터뷰
	개인정보 흐름 분석	대상 시스템에 대한 개인정보 취급 현황 산출물 타당성 및 운영 시스템 검토 대상 시스템에 대한 개인정보 흐름 관련 산출물 타당성 및 운영 시스템 검토	개인정보취급 업무표 업무 흐름도 개인정보 흐름표 개인정보 흐름도 시스템 구성도 담당자 인터뷰
평가	평가 수준 진단	대상 시스템에 대해 평가영역 별로 평가항목에 따라 평가	대상기관의 영향평가 항목 점검표 확인 영향평가항목점검표를 기준으로 영향평가 수행
	위험평가	대상 시스템에 대해 평가 및 침해요인에 따른 위험도를 산정	담당자 인터뷰, 영향평가 항목점검표 및 개인정보 흐름분석을 통한 위험평가 실시

단계		수행 내용	평가방법
	개선방안 도출	대상 시스템에 대한 침해요인별 위험도 측정결과에 대한 개선방안 수립	평가기관의 개인정보 침해요인별 개선방안 작성
보고	개선(이행) 계획 수립	대상 시스템에서 도출된 개인정보 침해요소 및 개선방안에 대해 위험도가 높은 순서로 개선방안에 대한 개선계획 수립	담당자와 개선계획 일정 인터뷰 평가기관의 개인정보 개선계획 수립
	PIA보고서 작성	영향평가 결과보고서 작성	평가기관의 영향평가 결과보고서 작성

[표3] 영향평가 수행절차

- 주요 평가사항
  - 당해 사업이 개인정보보호와 관련된 법적인 요건을 만족하는지 여부
  - 취급하는 개인정보에 대해 개인정보 생명 주기에 침해우려 발생 가능성 여부
  - 영향평가 점검표 기준으로 영향평가 결과 주요 침해사항 여부

- 평가기준 및 평가항목
  - 영향평가 수행 안내서 참고
  - 영향평가 수행 방법론((주)가나다PIA기관의 PIA 방법론)
  - 점검표 평가항목 기준으로 침해요인 분석 후 개선계획 수립

- 자료수집 및 분석 계획
  - 영향평가팀이 대상기관의 자료요청목록 요청 및 확인 검토
  - 대상기관의 부서별 요청항목

부서명	담당자	요청사항	비고
○○○ 시스템운영과	오○○	- 개인정보보호책임자의 수행업무 확인 - 영향평가 점검내용 검토	면담
○○○ 시스템운영과	김○○	- 대상기관 개인정보보호관리체계 관련 자료 제공 - 네트워크 및 시스템 구성도, 정보보호시스템 구성 내역, 기술적, 물리적 보호대책 수립 현황 - 영향평가 점검내용 검토	자료수집, 면담
○○○ 총무과	김○○	- CCTV 설치, 운영 현황 확인	자료수집, 면담
○○소프트웨어 (운영수탁기관)	박○○	- 시스템 운영 현황 확인	자료수집, 면담

[표4] 자료수집 및 면담대상 현황

- 평가결과 처리
  - 도출된 침해요인에 대해 개선방안 수립 및 사업기간 내 개선조치 가능한 사항에 대해서는 개선조치를 이행하고, 중장기적으로 이행해야 할 과제는 개선계획을 수립
  - 영향평가 결과보고서를 작성하여, 대상기관의 장에게 공문으로 제출(단계별 산출물은 전자파일로 별도 제출함)

5) 평가 기준

- 영향평가 수행안내서 "영향평가 항목"과 ABC공공기관의 개인정보보호 현황을 고려하여 ○개 평가영역, ○○개 평가분야, ○개 평가항목을 기준으로 함

평가영역	평가분야	세부분야	비고
Ⅰ. 대상기관 개인정보 보호관리 체계	1.1 개인정보보호조직	개인정보보호 책임자의 지정	
		개인정보보호책임자 역할수행	
	1.2 개인정보보호 계획	내부 관리계획 수립	
		개인정보보호 연간 계획 수립	
	1.3 개인정보 침해대응	침해사고 신고방법 안내	
		유출사고 대응	
	1.4 정보주체 권리보장	정보주체 권리보장 절차 수립	
		정보주체 권리보장 방법 안내	
Ⅱ. 대상시스템의 개인정보보호 관리체계	2.1 개인정보취급자 관리	개인정보취급자 지정	
		개인정보취급자 관리·감독	
	2.2 개인정보파일 관리	개인정보파일 대장 관리	
		개인정보파일 등록	
	2.3 개인정보 처리방침	개인정보 처리방침의 공개	
		개인정보 처리방침의 작성	
Ⅲ. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성	
		동의받는 방법의 적절성	
	3.2 보유	보유기간 산정	
	3.3 이용·제공	개인정보 제공의 적합성	
		목적 외 이용·제공 제한	
		제공시 안전성 확보	

평가영역	평가분야	세부분야	비고
	3.4 위탁	위탁사실 공개	
		위탁 계약	
		수탁사 관리·감독	
	3.5 파기	파기 계획 수립	
		분리보관 계획 수립	
		파기대장 작성	
IV. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	계정 관리	
		인증 관리	
		권한 관리	
	4.2 접근통제	접근통제 조치	
		인터넷 홈페이지 보호조치	
		업무용 모바일기기 보호조치	
	4.3 개인정보의 암호화	저장 시 암호화	
		전송 시 암호화	
	4.4 접속기록의 보관 및 점검	접속기록 보관	
		접속기록 점검	
		접속기록 보관 및 백업	
	4.5 악성프로그램 등 방지	백신 설치 및 운영	
		보안업데이트 적용	
	4.6 물리적 접근 방지	출입통제 절차 수립	
		반출·입 통제절차 수립	
	4.7 개인정보의 파기	안전한 파기	
	4.8 기타 기술적 보호조치	개발환경 통제	
		개인정보 처리화면 보안	
		출력 시 보호조치	
	4.9 개인정보 처리구역보호조치	보호구역 지정	

평가영역	평가분야	세부분야	비고
V. 특정IT 기술 활용 시 개인정보보호	5.1 CCTV	CCTV 설치시 의견수렴	
		CCTV 설치 안내	
		CCTV 사용 제한	
		CCTV 설치 및 관리에 대한 위탁	
	5.2 RFID	RFID 이용자 안내	
		RFID태그부착 및 제거	
	5.3 바이오정보	원본정보 보관 시 보호조치	
	5.4 위치정보	개인위치정보 수집 동의	
		개인위치정보 제공시 안내사항	

[표5] 평가기준

6) 영향평가 점검항목 조정

- 점검항목 조정 요약

구분	점검항목 수				비고
	조정전	추가	제외	조정후	
대상기관 관리체계	9	1	-	10	
대상시스템 관리체계	6	-	-	6	
처리단계별 보호조치	21	-	-	21	
기술적 보호조치	33	-	1	32	
특정 IT 기술 활용	16	-	11	5	
합계	85	1	12	74	

[표6] 점검항목 조정 요약표

- 점검항목 조정 요약

구분	추가 또는 제외 항목		추가 또는 제외 사유
	코드	내용	
항목 추가	1.2.4	대상기관은 개인정보보호계획에 중요한 변경이 있는 경우 이를 즉시 반영하여 개인정보보호 계획을 수정, 시행하고 수정이력을 관리하고 있습니까?	개인정보보호계획 중 중요한 변경이 어떤 것인지를 파악할 필요가 있고, 표준 개인정보 보호지침에서 이력관리를 규정하고 있으므로 추가
	-	-	-
항목 제외	4.2.6	개인정보를 처리하는 업무용 모바일기기의 분실·도난 등으로 개인정보가 유출되지 않도록 모바일 기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?	대상 시스템은 업무용 모바일 기기를 사용하지 않으므로, 해당 항목은 해당 사항이 없음
	-	-	-

[표7] 점검항목 조정 내역 현황표

1.3 대상 시스템의 개요

1) 사업명

- ABC공공기관 홈페이지 구축

2) 사업추진 목표

- ○○○ 정보 이용과 정보전달을 주로 담당하는 ○○ 홈페이지를 소통과 협업 기반의 정보 문화 융성의 환경을 제공하는 방식으로 개편하여 모든 ○○○정보가 공유·활성화 되는 웹사이트를 목표로 함
- 서비스 플랫폼 고도화를 통해 대국민서비스 확장·연계 시 유연성 및 확장성, 안전성 확보

3) 사업 추진 일정

- 2019.○○.○○ ~ 2020.○○.○○

4) 사업 추진 예산

- 000,000,000원(VAT 포함)

5) 사업내용

가) 추진배경 및 필요성

- 대국민이 주로 이용하는 홈페이지의 기능 및 디자인 고도화 필요
  - ○○○ 정보 이용을 위한 홈페이지 이용 관문(Portal) 및 게시판 위주의 일방적 정보 전달 역할의 웹사이트에서, ○○ 관련 업무 수행의 효율화 정보 공유까지 가능한 "민원 서비스" 중심의 포털로 개선
  - ○○○ 정보에 대한 신속한 전달 및 대국민 대상 사용 편리성 강화를 위한 웹사이트로의 개편

- 정보 소통 방식 개선
  - "알림", "전달" 위주의 단방향 소통을 "참여", "공유"의 양방향 소통으로 확대 개편
  - 소통과 협업 기반의 새로운 정보화 환경을 제공하여 ○○○○ 문화 개선 유도
  - 스마트(Smart)하게 정보를 공유하는 사회적 패러다임 적용

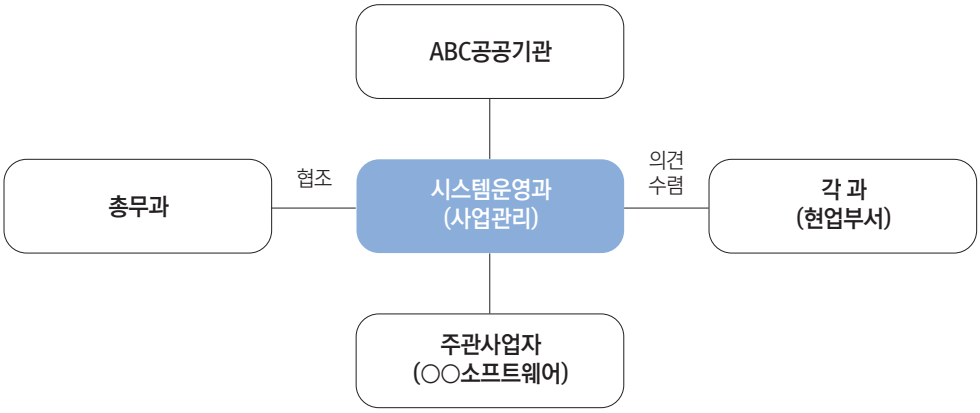
- 온라인 정보이용 환경의 급격한 변화
  - 급변하는 정보화(IT) 기술을 쉽게 수용할 수 있도록 플랫폼에 종속되지 않는 유연성과 확장성을 갖는 웹사이트로 강화
  - 정보의 재사용 및 공개를 위하여 전자정부 표준 프레임워크를 활용한 표준화

나) 사업추진 범위

- 상단 메뉴(Global Navigation Bar, GNB) 정보 체계 변경
- 대국민서비스 통합 홈페이지 디자인 개선
- 온라인 민원서비스 제공 기능 구축
- 개인별 맞춤 서비스를 위한 개인화 서비스 기능 개발
- 통합 홈페이지 효율적 운영을 위한 콘텐츠 관리 기능 고도화
- 통합 로그인(SSO: Single Sign On) 적용

다) 사업 추진 체계

- 사업추진 조직도



구분		역할 및 책임
시스템운영과	전담기관	● 사업진행 총괄 ● 사업추진관련 기관간의 의견 조정
ABC공공기관 (각 과)	지원부서	● 서비스 이용자 ● 요구사항제시 ● 기능 검증 ● 통합 시험 참여
(주)○○소프트웨어	주관사업자	● 사업 이행의 총괄적 책임 ● 사업관리 및 품질관리 ● 서비스 모니터링 및 안정적 운영 ● 시스템 운영 및 서비스 기능 개선 ● 운영산출물 작성 ● ○○ 및 기술지원

1.4 영향평가 수행인력 및 비용

1) 영향평가 투입인력

단계	평가분야	소요 일수	투입인원		세부일정	투입공수
사전 분석	영향평가 필요성 검토	3 일	3 명	특급 3	2020.○○.○○ ~ 2020.○○.○○	○○MD
	팀 구성 및 운영계획서 작성					
	평가 계획 수립					
영향 평가	평가자료 수집 및 분석	2 일	3 명	특급 3	2020.○○.○○ ~ 2020.○○.○○	○○MD
	개인정보 흐름 분석	9 일	3 명	특급 3	2020.○○.○○ ~ 2020.○○.○○	○○MD
	영향평가 평가항목 작성 및 점검	15 일	3 명	특급 3	2020.○○.○○ ~ 2020.○○.○○	○○MD
	침해요인 분석 및 위험도 산정					
	통제항목 도출 및 개선방안 도출	6 일	4 명	특급 4	2020.○○.○○ ~ 2020.○○.○○	○○MD
결과 정리	개선계획 및 결과 보고서 작성	4 일	4 명	특급 4	2020.○○.○○ ~ 2020.○○.○○	○○MD
	결과보고서 협의 및 조정					
	영향평가 결과보고서 제출	상주 컨설팅 후 10일 이내 보고서 제출				
영향평가 투입 공수		총 ○○ MD				

[표8] 영향평가 수행인력 투입내역

※ 투입판단근거 : 해당시스템의 규모·복잡도 등을 고려하였음

=> 운영사업비 ○○만원, 개인정보 파일 수○, 업무 수○, 개인정보 취급자 수 ○○명(홈페이지 : ○○명, 통합회원관리시스템 ○○명)

2) 영향평가 수행비용

- 수행비용 : OO만원(₩○○) 부가세 포함

구분	기술자구분	등급	노임단가	투입인원(명)	투입공수(M/M)	적용금액	비고
인건비	PM	특급	7,474,570	1	0.75		
	컨설턴트	특급	7,474,570	1	1.50		
		특급	7,474,570	1	1.00		
		특급	7,474,570	1	0.25		
	소계				3.5		
제경비			인건비의 1%				
기술료			(인건비+제경비)의 1%				
소계							
부가세							
용역비 합계							

[표9] 영향평가 수행비용

1.5 개인정보파일 운용의 목적

- ABC공공기관 홈페이지 이용자 관리 및 맞춤 서비스 제공

2. 개인정보파일의 개요

2.1 개인정보파일의 개요

개인정보파일을 운용하는 공공기관의 명칭		ABC공공기관		
부서명		시스템운영과	취급담당자	이○○
업무분야		○○○		
개인정보파일의 명칭		ABC공공기관 통합회원명부		
개인정보파일의 운영 근거		정보주체동의(홈페이지 이용약관)		
개인정보파일의 운영 목적		○○○ 이용자 관리 및 맞춤정보서비스 제공		
개인정보파일에 기록되는 개인정보의 항목		아이디, 비밀번호, 성명, 성별, 생년월일, 전화번호, 휴대폰번호, 이메일주소, 주소, 직업, 장애여부, ○○○, ○○○이용목적, 관심분야, ○○○(학교명,학년,반), ○○○성명		
개인정보의 처리방법		온라인 수집 (홈페이지 회원신청, 전자접수 등), 기타		
개인정보의 보유기간		2년 (단, 가입시 본인이 유효기간 설정이 가능하며 미 설정시 기본 2년으로 설정됨)		
개인정보를통상적 또는반복적으로 제공하는 경우	제공받는자	해당 없음		
	근거	해당 없음		
	개인정보의범위	해당 없음		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		○○명		
해당 공공기관에서개인정보 처리 관련 업무를 담당하는 부서	범위	해당 업무부서의 담당자와 시스템 관리자만이 접근하여 활용할 수 있다.		
	공동사용부서	○○정보과		
개인정보의 열람 요구를 접수, 처리하는 부서		서울특별시 ○○구 ○○로 ABC공공기관 시스템운영과		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	개인정보의범위	비밀번호		
	사유	사용자 인증과 관련된 정보로 비밀 유지 필요		

[표10] 개인정보파일 개요

3. 개인정보 흐름분석

3.1 필요성 검토 결과

- 홈페이지 시스템의 경우 약 ○○명의 회원 정보를 보유하고 있으며 고유식별정보를 처리하지 않고, 타 기관과 연계를 계획하지 않고 있으나, 홈페이지 회원은 향후에도 지속적으로 증가할 것으로 추정함

No	질문	Y/N 또는 해당없음	내용
1	5만 명 이상의 정보주체에 관한 민감 정보 또는 고유 식별 정보의 처리가 수반 또는 수반될 것으로 예상됩니까?	N	
2	해당 공공기관 내부 또는 외부에서 구축 · 운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계한 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함 또는 포함될 것으로 예상됩니까?	N	
3	100만 명 이상의 정보주체에 관한 개인정보파일을 처리 또는 처리가 예상됩니까?	Y	
4	법 제33조 제1항에 따른 영향평가를 받은 후에 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려고 합니까?	N	

[표11] 영향평가 의무대상 여부 확인표

3.2 평가자료 수집

1) 평가자료 수집 목적 및 종료

- 영향평가의 수행에 앞서 평가 대상 및 개인정보 정책 환경을 분석하기 위한 관련 자료를 수집함.
- 분석 대상 자료는 기관 내 · 외부 개인정보 보호 관련 규정 및 정책 환경 등을 분석하기 위해 개인정보 보호와 관련한 ① 내부 정책자료, ② 외부 정책자료, ③ 대상시스템 설명자료 등으로 구분함

2) 내부정책 자료

- 조직 체계 자료

수집목적	수집자료	수집기관
기관 내부의 개인정보보호 체계, 규정, 조직현황 파악	- 해당기관 조직도, 업무분장표, 직무기술서 - 개인정보보호조직 조직도 - 개인정보보호 내부 관리계획, 개인정보보호지침 - 연간 개인정보보호 활동계획서 및 결과서 - 개인정보처리방침	ABC공공기관

[표12] 조직, 체계자료 목록

- 인적보안 및 교육자료

수집목적	수집자료	수집기관
기관 내부의 개인정보취급자 및 위탁업체에 대한 내부규정 및 관리·교육체계 파악조직 현황 파악	- 개인정보보호 교육계획서(년간, 건별)(개인정보취급자, 개인정보 보호책임자 등) - 개인정보보호 교육결과서(과정, 참석자 식별가능한 결과자료) - 개인정보 취급자 명단(기관 전체 및 대상 시스템) - 개인정보처리 위탁업체/제3자 목록	ABC공공기관

[표13] 인적 통제, 교육자료 목록

- 시스템 구성 및 보안 관련 자료

수집목적	수집자료	수집기관
시스템 구조와 연계된 개인정보보호기술 현황 파악	- 시스템 배치도 - 네트워크/시스템 구성도 - 전산실 출입관리대장 - CCTV 관리대장 - 개발보안규정(또는 지침, 가이드	ABC공공기관

[표14] 정보보안 자료 목록

3) 외부정책 자료

- 대상기관 관련 법률

수집목적	수집자료	수집기관
개인정보보호 관련 정책 및 법률 등 환경 분석	- 개인정보 보호법/시행령/개인정보 처리방법에 관한 고시 - 개인정보의 안전성 확보조치 기준 - 공공기관 개인정보보호 기본 지침	㈜영향평가팀

[표15] 공공기관 관련 법률 목록

- 대상기관 개인정보보호 관련 지침

수집목적	수집자료	수집기관
소속기관의 규정 및 지침 분석	- 상급기관의 개인정보보호 규정/지침/가이드	ABC공공기관

[표16] 대상기관 개인정보보호 관련 법률 목록

4) 대상시스템 설명 자료

- 사업관리 자료

수집목적	수집자료	수집기관
정보시스템에 의하여 수집되는 개인정보의 양과 범위가 사업 수행을 위해 적절한지 파악	- 제안요청서(RFP) - 프로젝트 계약서 - 사업수행계획서	ABC공공기관

[표17] 사업관리 자료 목록

- 외부연계 자료

수집목적	수집자료	수집기관
정보시스템의 외부 연계 여부 파악	- 인터페이스 기관 목록 - 인터페이스 목록 - 인터페이스 설계서	ABC공공기관

[표18] 외부연계 자료 목록

- 시스템 관련 자료

수집목적	수집자료	수집기관
시스템 개발(운영) 분석	- 업무흐름도 - 메뉴 구성도 - 요구사항 정의서, 화면 설계서, ERD - 유스케이스 다이어그램, 시퀀스 다이어그램	ABC공공기관

[표19] 개발 및 운영 산출물 목록

3.3 업무흐름 분석

1) 목적

- 본 사업의 모든 업무가 개인정보를 취급하는 것은 아니므로, 평가 대상 사업의 업무를 분석하여 개인정보 취급이 수반되는 업무를 구분하고 각 업무에서 취급하는 개인정보를 식별함

2) 정보주체

- ABC공공기관에서 제공하는 서비스를 이용하기 위하여 홈페이지 통합회원으로 가입한 이용자

3) 개인정보취급자

- ABC공공기관 홈페이지를 통하여 접수, 처리하는 신청업무 담당자(내부직원, 임시직, 계약직 포함)
- ABC공공기관 홈페이지 통합회원관리시스템을 통하여 회원 조회, 아이디/비밀번호 찾기 등 이용자 민원대응 담당자(내부직원, 임시직, 계약직 포함)
- ABC공공기관으로부터 홈페이지 및 통합회원관리시스템 운영, 유지보수 업무 수탁기관 직원

4) 시스템 평가 범위

분 야		홈페이지 시스템
홈페이지	○○○ ○○관리	○○ 신청 접수, 승인, 처리결과 조회
	○○ 신청관리	○○ 참가 신청 접수, 승인, 처리결과 조회
통합회원 관리시스템	회원관리	홈페이지 통합회원 가입, 회원정보 조회, 통합회원 전환 및 탈퇴

[표20] 시스템 평가 범위

5) 개인정보 취급 업무표

- ABC공공기관 홈페이지 시스템의 개인정보 취급 업무는 아래와 같음
- ABC공공기관 홈페이지 시스템은 고유식별정보를 처리하지 않음

평가업무	취급 개인정보	주관부서	개인정보건수 (고유식별정보건수)	개인정보 영향도
회원관리	필수: 성명, 생년월일, 성별, 장애구분, 회원ID, 비밀번호, 주소, 직업, 전화번호, 휴대전화, 이메일 선택: ○○○, 장애인증명파일, ○○○성명, 관심분야, ○○○, 인근○○○정보	시스템 운영과	○○	5
○○ 신청관리	필수: 성명(신청자), 소속(단체명), 인솔자, 전화번호, 이메일, 주소 선택: 휴대전화	○○ 홍보팀	본관: ○○ ○○: ○○	3

[표21] 개인정보 취급 업무표

6) 개인정보 현황표

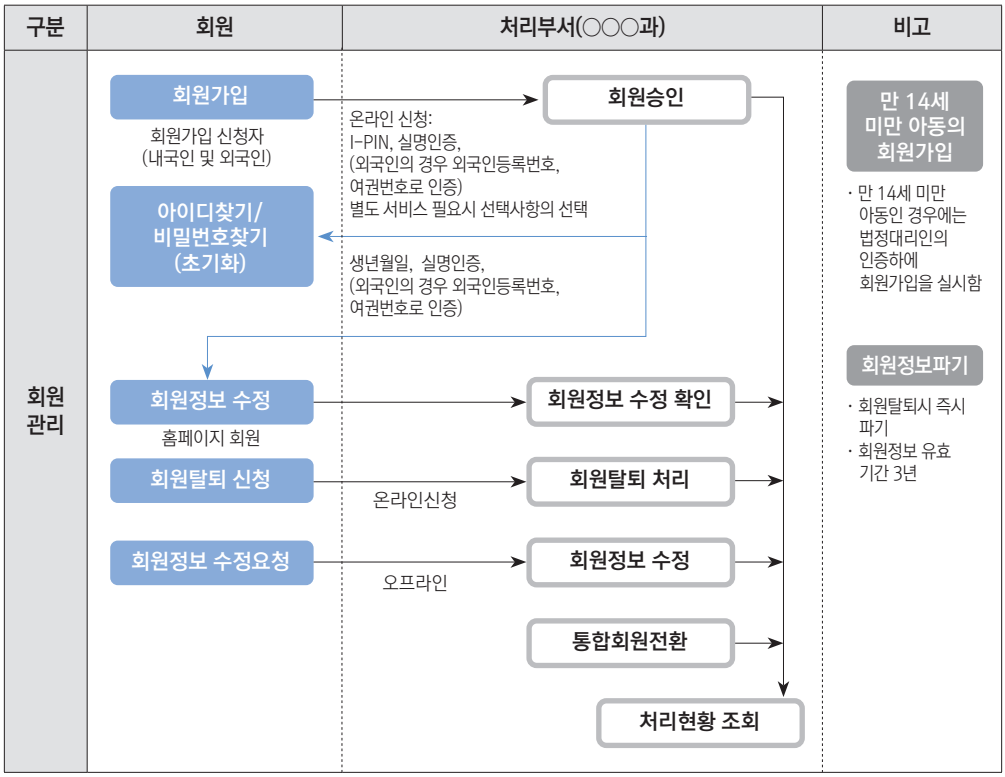
- ABC공공기관 대표 홈페이지 시스템의 개인정보 현황표는 아래와 같음

평가 업무	개인정보 처리항	개인정보 세부항목	수집근거	필수/ 선택	수집목적
회원 관리	성명	-	정보주체 동의	필수	본인확인
	생년월일	-	정보주체 동의	필수	본인확인
	성별	-	정보주체 동의	필수	성별구분
	장애구분	-	시각장애인:저작권법 제33조(시각장애인 등을 위한 복제 등) 기타: 정보주체 동의	선택	맞춤형서비스등의 개인화서비스와 이용자 서비스 개발을 통한 이용자의 편익 증진 (장애인인 경우 본인 동의하에 선택적으로 수집)
	회원ID	-	정보주체 동의	필수	본인확인
	비밀번호	-	정보주체 동의	필수	본인인증
	....	....	....	....	....

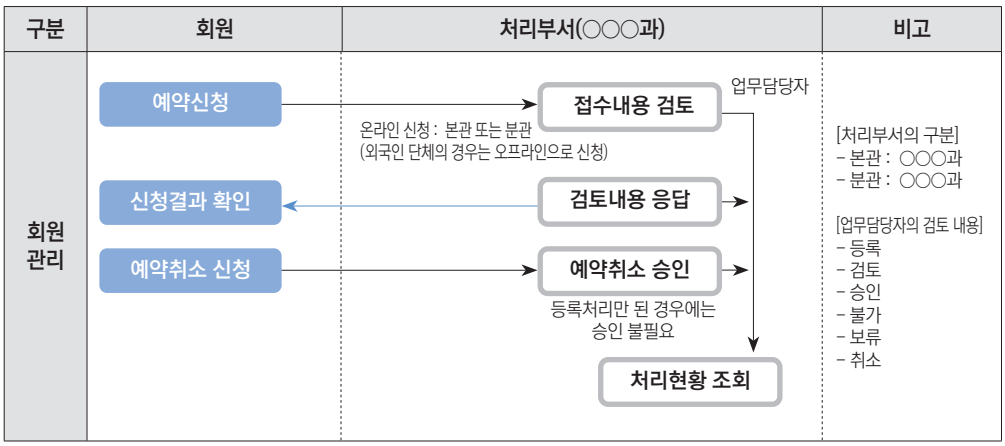
[표22] 개인정보 현황표

3.4 업무흐름도

- ABC공공기관 홈페이지 시스템의 업무흐름도는 다음 그림과 같음



[그림 7] 업무흐름도 – 회원관리



[그림 8] 업무흐름도 – ○○신청관리

3.5 개인정보 흐름표

- ABC공공기관 홈페이지 시스템 **수집단계** 개인정보 흐름은 아래와 같음

No	업무명	수집					
		수집항목	수집경로	수집대상	수집주기	수집담당자	수집근거
1-1	회원관리 (회원가입)	필수: 성명, 생년월일, 성별, 장애구분, 회원ID, 비밀번호, 주소, 직업, 전화번호, 휴대전화, 이메일, 선택: ○○○,장애인증명파일, ○○○성명, 관심분야, ○○○, 인근○○○정보	홈페이지 (온라인)	정보주체	수시	홈페이지 담당자	정보주체 동의
1-2	회원관리 (회원정보 수정)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
1-3	회원관리 (아이디/ 비밀번호 찾기)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
1-4	회원관리(회원탈퇴)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
2	○○ 신청관리	필수: 소속(단체명), 인솔자, 휴대전화	홈페이지 (온라인) 신청서 (오프라인)	정보주체	수시	○○업무 담당자	정보주체 동의

[표23] 개인정보 흐름표(수집단계)

- ABC공공기관 홈페이지 시스템 **보유·이용단계** 개인정보 흐름은 아래와 같음

No	업무명	보유, 이용					
		보유 형태	암호화 항목	이용항목	이용목적	개인정보 취급자	이용방법
1-1	회원관리 (회원가입)	DB	비밀번호 (SHA- 256)	필수: 성명, 생년월일, 성별, 장애구분, 회원ID, 비밀번호, 주소, 직업, 전화번호, 휴대전화, 이메일, 선택: ○○○, 장애인증명파일, ○○○성명, 관심분야, ○○○, 인근○○○정보	담당자가 회원 정보를 관리	홈페이지 담당자	개인 PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 회원정보 조회
1-2	회원관리 (회원정보 수정)	DB	비밀번호 (SHA- 256)	필수: 성명, 생년월일, 성별, 장애구분, 회원ID, 비밀번호, 주소, 직업, 전화번호, 휴대전화, 이메일	회원이 자신의 개인정보를 수정하고 조회	홈페이지 회원	개인PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 수정 및 정보조회
1-3	회원관리 (아이디/ 비밀번호 찾기)	DB	비밀번호 (SHA- 256)	필수: 성명, 생년월일, 회원ID, 비밀번호, 전화번호, 휴대전화, 이메일	회원이 자신의 아이디 또는 비밀번호를 조회	홈페이지 회원	개인 PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 정보 조회 (비밀번호는 신규로 재입력 필요)

No	업무명	보유, 이용					
		보유 형태	암호화 항목	이용항목	이용목적	개인정보 취급자	이용방법
1-4	회원관리 (회원탈퇴)	DB	비밀번호 (SHA- 256)	필수: 회원ID, 성명, 비밀번호	회원이 자신의 회원탈퇴처리	홈페이지 회원	개인 PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리
2	○○ 신청관리	DB, 문서		필수:성명(신청자),전화번호, 이메일,주소,소속(단체명),인솔자, 선택:휴대전화	○○ 신청자에 대한 정보 관리	○○업무 담당자	개인 PC를 이용하여 홈페이지에 접속한 후 해당 메뉴 선택하여 처리

[표24] 개인정보 흐름표(보유·이용단계)

- ABC공공기관 홈페이지 시스템 **제공·위탁단계** 개인정보 흐름은 아래와 같음

No	업무명	제공·위탁						
		제공자	수신자	제공정보	제공방법	제공목적	제공시 암호화	제공근거
1-1	회원관리 (회원가입)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
1-2	회원관리 (회원정보 수정)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
1-3	회원관리 (아이디/비밀번호 찾기)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
1-4	회원관리 (회원탈퇴)	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음
2	○○ 신청관리	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음	해당없음

[표25] 개인정보 흐름표(제공, 위탁단계)

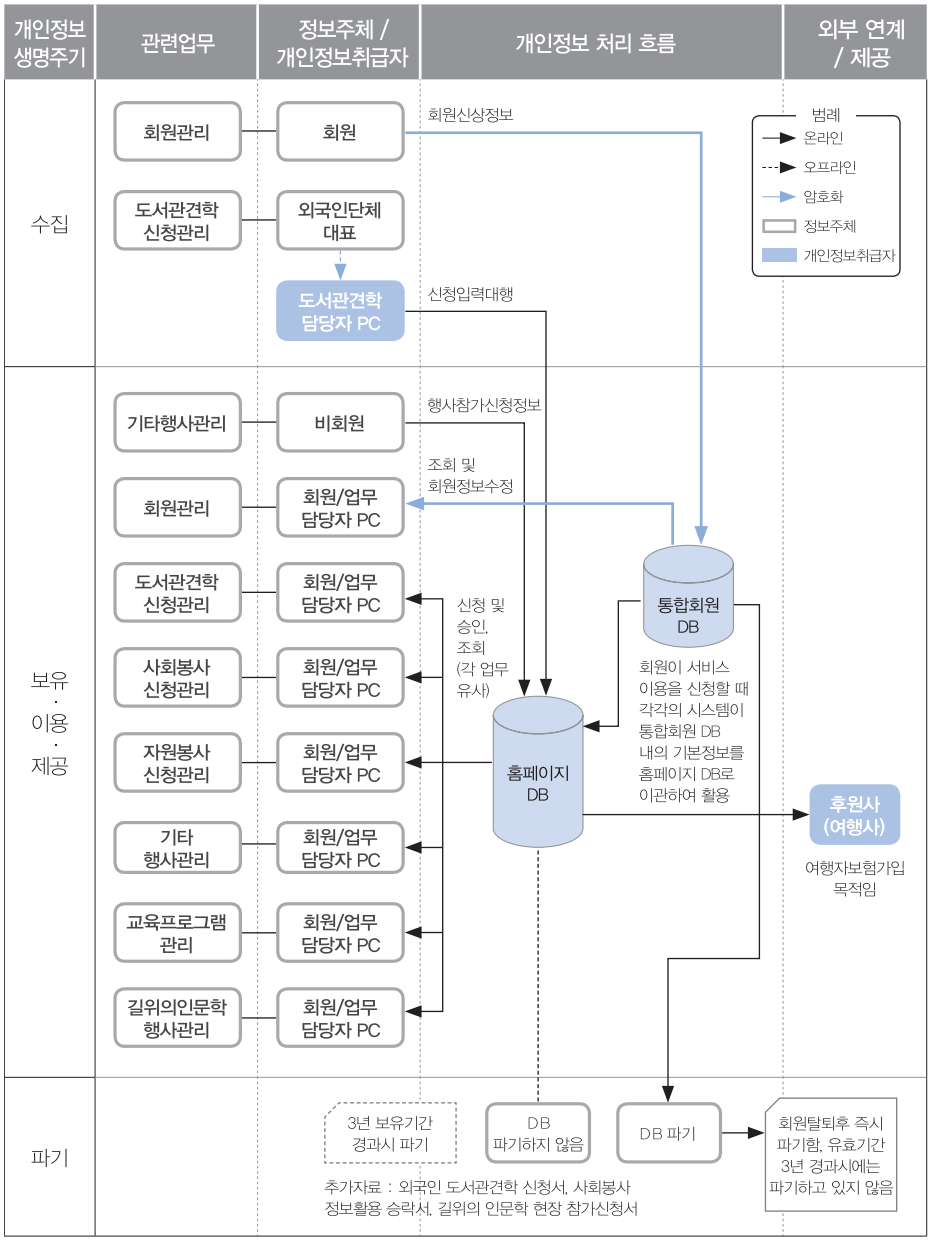
- ABC공공기관 홈페이지 시스템 **파기단계** 개인정보 흐름은 아래와 같음

No	업무명	파기			
		보관기간	파기담당자	파기절차	분리보관
1-1	회원관리 (회원가입)	회원탈퇴 후 지체없이 삭제 또는 최대3년	홈페이지 담당자	목적 달성시 테이블에서 해당 레코드 삭제. 그러나 기간경과 후 파기하지 않음	
1-2	회원관리 (회원정보수정)	-	-	-	
1-3	회원관리 (아이디/비밀번호 찾기)	-	-	-	
1-4	회원관리 (회원탈퇴)	회원탈퇴 후 지체없이 삭제	홈페이지 담당자	테이블에서 해당 레코드 삭제	
2	○○ 신청관리	DB:보관기간 미설정 신청서:3년	○○업무 담당자	DB :파기하지 않음 신청서 기간경과 후 분쇄기로 파기	

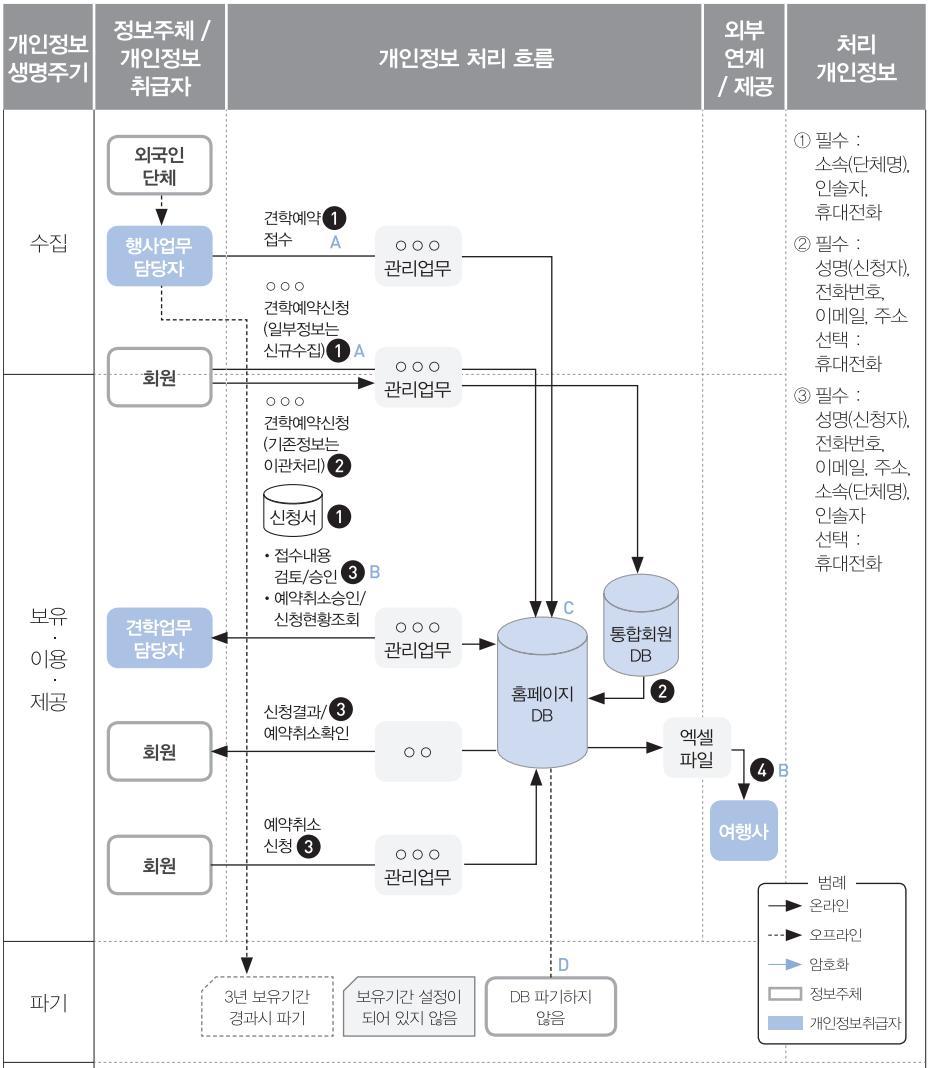
[표26] 개인정보 흐름표(파기단계)

3.6 개인정보 흐름도

- ABC공공기관 홈페이지 시스템의 개인정보 흐름도는 아래와 같음



[그림 13] 개인정보흐름도 – 총괄

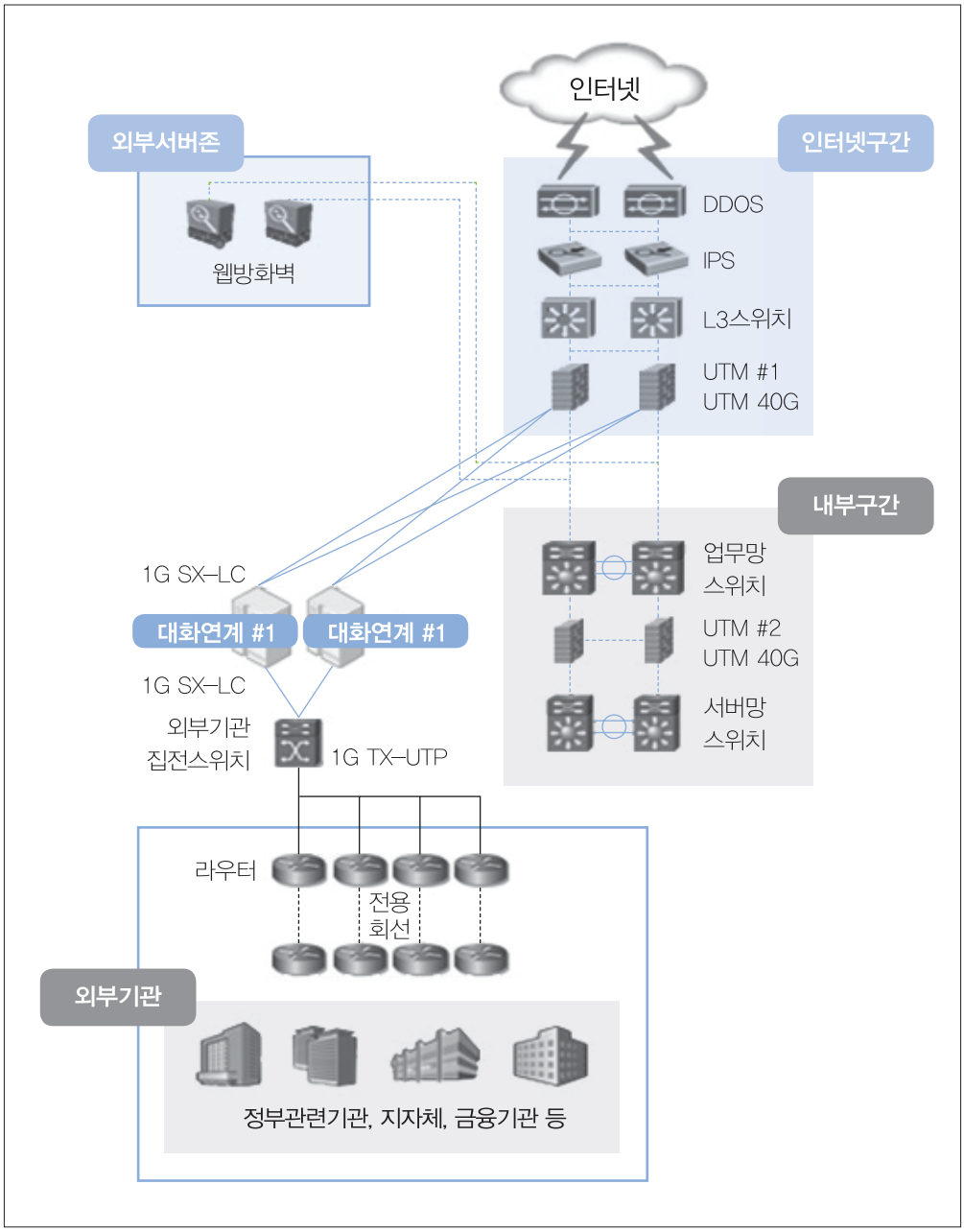


주요 업무흐름 설명	▶ 신청자는 ○○ 견학신청 화면을 통하여 본관 또는 분관의 견학을 신청함(외국인단체의 경우는 ○○○ 견학 담당자에게 견학참가신청을 의뢰하면 담당자가 자신의 아이디로 신청을 대행함 ▶ ○○○ 업무 담당자는 신청내용을 검토하여 검토결과를 등록함(검토결과–검토, 승인, 불가, 보류, 취소) ▶ 신청자는 '○○'를 통하여 신청결과를 확인함 ▶ 예약을 취소할 경우에는 승인이 된 경우에는 ○○○ 견학 업무 담당자에게 취소를 의뢰하여 취소처리를 함
우려사항	A. 신규로 수집되는 일부 개인정보가 정보주체의 동의 없이 수집되고 있음(3.1.1) B. 강화된 비밀번호 조합규칙을 적용하고 있지 않아 제3자가 비밀번호를 알아낼 가능성이 존재함(4.1.2) C. 홈페이지DB에 저장된 개인정보에 대해서는 별도의 처리로그가 기록되지 않아 침해사고 발생 시 추적성 확보가 되지 않음(4.4.1) D. 개인정보의 보유기간이 설정되어 있지 않고 파기되지 않아 개인정보의 유출과 오용 가능성이 존재함(3.5.1)

[그림 14] 업무별 개인정보흐름도 – OOO관리

3.7 네트워크 구성도

- ABC공공기관 홈페이지 시스템의 네트워크 구성도는 아래와 같음



[그림 21] 네트워크 구성도

3.8 정보보호시스템 목록

- ABC공공기관 홈페이지 시스템 관리 시 적용하고 있는 정보보호시스템 목록은 아래와 같음

유형	적용 솔루션명	목적 및 용도	적용 대상	본 사업 범위 여부
방화벽	○○○	외부로부터 내부망을 보호하기 위한 장비로써 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 외부로부터 유해정보유입을 차단하기 위한 장비	Main, 내부망, 서버팜, 본관서버팜, 외부이용자망, 업무망	기 운영중
웹방화벽	○○○	웹서버에 대해 HTTP 서비스 해킹방어	DMZ	기 운영중
IPS	○○○	트래픽 모니터링과 공격유형 분석을 통해 침입시도나 인가되지 않은 행위와 같은 유해 트래픽을 탐지 및 차단	Main, 외부이용자망	기 운영중
UTM	○○○	트래픽 모니터링과 공격유형 분석을 통해 침입시도나 인가되지 않은 행위와 같은 유해 트래픽을 탐지 및 차단	외부이용자망	기 운영중
무선침입방지 시스템	○○○	트래픽 모니터링과 공격유형 분석을 통해 침입시도나 인가되지 않은 행위와 같은 유해 트래픽을 탐지 및 방어	외부이용자망	기 운영중
DDoS 방어시스템	○○○	외부로부터의 DDoS공격차단	Main	기 운영중

[표27] 정보보호시스템 목록

4. 영향평가 결과

4.1 영향평가 항목점검 결과

- ABC공공기관 홈페이지 시스템 평가영역은 총 5개 영역으로 구성되며, 영향평가 결과, 전체 이행율은 80%임
  ※전체이행율 = (51+13*0.5)/(51+13+8) = 80%
- 대상기관의 개인정보보호 관리체계 영역은 개인정보보호조직, 개인정보보호 계획 등 대부분의 평가분야에서 미흡한 사항이 발견됨
- 대상시스템의 개인정보보호 관리체계 영역은 개인정보취급자 지정이 미흡한 것으로 평가함
- 개인정보 처리단계별 보호 영역은 수집, 보유·저장, 이용·제공, 파기 등 전 분야에서 취약사항이 있는 것으로 평가함
- 대상시스템의 기술적 보호조치 영역은 양호한 상태로 평가됨
- 특정 IT기술 활용 영역에서 CCTV 활용분야는 미흡한 상황이 발견됨

범례 [Y(이행), P(부분이행), N(미이행), N/A(해당없음)]

평가영역	평가분야(전체)	점검 개수	점검 결과				
			Y	P	N	N/A	이행율
1. 대상기관 개인정보 보호 관리체계	1.1 개인정보보호 조직	2	1	1	0	0	75%
	1.2 개인정보보호 계획	4	1	1	2	0	38%
	1.3 개인정보 침해대응	2	2	0	0	0	100%
	1.4 정보주체 권리보장	2	2	0	0	0	100%
2. 대상시스템의 개인 정보보호 관리체계	2.1 개인정보취급자 관리	2	0	2	0	0	50%
	2.2 개인정보파일 관리	2	2	0	0	0	100%
	2.3 개인정보 처리방침	2	2	0	0	0	100%
3. 개인정보 처리단계별 보호조치	3.1 수집	7	5	0	2	0	71%
	3.2 보유	1	1	0	0	0	100%
	3.3 이용·제공	7	2	2	1	2	60%
	3.4 위탁	3	1	2	0	0	67%
	3.5 파기	3	2	0	1	0	67%
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	10	9	1	0	0	95%
	4.2 접근통제	5	5	0	0	0	100%
	4.3 개인정보의 암호화	3	2	1	0	0	83%
	4.4 접속기록의 보관 및 점검	3	2	10	0	0	83%
	4.5 악성프로그램 등 방지	2	1	0	1	0	50%
	4.6 물리적 접근방지	2	2	0	0	0	100%
	4.7 개인정보의 파기	1	1	0	0	0	100%
	4.8 기타 기술적 보호조치	3	2	1	0	0	83%
	4.9 개인정보처리구역 보호	3	3	0	0	0	100%
5. 특정IT기술 활용시 개인정보보호	5.1 CCTV	5	3	1	1	0	70%
	5.2 RFID	0	0	0	0	0	-
	5.3 바이오정보	0	0	0	0	0	-
	5.4 위치정보	0	0	0	0	0	-
합계		74	51	13	8	2	80%

[표28] 평가분야별 이행 수준

- ABC공공기관 홈페이지 시스템 영향평가 항목점검 결과

질의문 코드	질의문	홈페이지 시스템				비고
		이행	부분 이행	미 이행	해당 없음	
1.1 개인정보보호 조직						
1.1.1	개인정보 보호책임자를 법령 기준에 따라 지정하고 있습니까?	○				
1.1.2	개인정보 보호책임자에게 법령 등이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?		○			
1.2 개인정보보호 계획						
1.2.1	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있습니까?	○				
1.2.2	개인정보보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 있습니까?			○		
1.2.3	개인정보보호 교육, 실태점검 등 개인정보보호 활동에 대한 연간 수행계획을 수립·시행하고 있습니까?		○			
1.2.4	대상기관은 개인정보보호계획에 중요한 변경이 있는 경우 이를 즉시 반영하여 개인정보보호계획을 수정, 시행하고 수정이력을 관리하고 있습니까?			○		추가 지표
1.3 개인정보 침해대응						
1.3.1	개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?	○				
1.3.2	개인정보 유출 신고·통지 절차, 긴급 연락체계, 사고대응 조직 구성 등을 포함한 개인정보 침해신고 대응절차를 수립하여 실시하고 있습니까?	○				
1.4 정보주체 권리보장						
1.4.1	개인정보 열람, 정정·삭제, 처리정지, 수집출처 고지 등 정보주체의 요구에 대한 처리절차를 수립하여 실시하고 있습니까?	○				
....	....					

[표29] 영향평가 항목점검 결과표

4.2 대상기관 개인정보보호 관리체계

1) 대상기관 개인정보보호 조직 분야 현황 및 침해요인 도출

- (1.1.2) 2020년 ABC공공기관 개인정보보호 시행계획(개인정보 내부 관리계획서) 'Ⅰ.현황 및 목표'에서 시스템운영과장을 개인정보보호책임자로 지정하고 있고, 개인정보 보호법령에서 정한 업무를 시행하고 있음. 기술적 보안관리지침(첨부4.개인정보보호규정)에서 개인정보보호총괄부서의 업무를 규정하고 있으나, 법령에서 정한 업무를 모두 포함하고 있지 않음

개인정보 침해 위험

개인정보보호책임자가 정보주체의 개인정보 보호를 위해 개인정보 보호법령에서 반드시 수행하도록 규정한 업무를 누락할 경우 관련 법령 조항을 준수하지 못하게 되며, 개인정보의 안전한 관리를 위한 조치가 미비될 위험이 있음

2) 대상기관 개인정보보호 계획 분야 현황 및 침해요인 도출

- (1.2.3) 2020년 ABC공공기관 개인정보보호 시행계획(개인정보 내부 관리계획서)에서 연간 개인정보 보호교육 계획을 수립하여 개인정보취급자를 대상으로 연 1회 개인정보보호 교육을 시행하도록 계획하고 있음. 하지만, 본사 대강당에서의 2020.5.20.에 집체교육으로 1회 수행하는 것으로만 되어 있어 전체 개인정보취급자(500명) 대비 강의장 좌석수(100석)가 많이 부족하여 전체 개인정보취급자의 참석이 어렵고, 나머지 인원에 대한 교육계획은 수립되어 있지 않음

개인정보 침해 위험

개인정보취급자 중에 개인정보보호 교육을 받지 않은 인원이 다수 발생하는 경우에, 개인정보 보호법에서 요구하는 개인정보취급자 관리감독 조항을 위반하여 처벌을 받을 수 있으며, 교육을 받지 못한 개인정보취급자의 경우 개인정보보호 관련 규정에 대한 이해 부족으로 개인정보보호 관련 법률 및 규정을 위반하게 될 위험이 있음

5. 위험 평가

5.1 위험 평가 개요

1) 위험평가 목적

- 영향평가 결과에서 도출된 침해위험을 기준으로 위험평가를 수행하고, 평가결과에 따라 효과적인 보호대책 수립을 목적으로 함

2) 위험도의 활용

- 영향평가 결과에서 도출된 침해요인들은 개선하여야 하며, 개선사항의 우선순위를 선정하는데 위험도 산정을 활용할 수 있음

3) 위험도 산정공식

- 영향평가 수행안내서에서는 개인정보 침해위험 요소의 위험도 산정공식을 아래와 같이 제시하고 있으므로, 본 사업에서는 이 공식을 적용함

위험도 = 자산 가치(영향도) + (침해요인 발생가능성 × 법적 준거성) × 2

- 개인정보 취급이 발생하는 업무와 해당 업무를 통해 취급되는 개인정보의 현황과 각 개인정보 항목의 조합 수준에 따른 영향도를 아래 표와 같이 구분하여 평가함

등급	조합설명	위험성	자산 가치	분류	개인정보 종류
1 등급	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	·정보주체의 경제적/사회적 손실을 야기하거나, 사생활을 현저하게 침해 ·범죄에 직접적으로 악용 가능 ·유출 시 민/형사상 법적 책임 부여 가능 및 대외 신임도 크게 저하	5	고유 식별 정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 ※「개인정보 보호법」제24조 및 동법 시행령 제19조
				민감 정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전자검사정보, 범죄경력정보 등 사생활을 현저하게 침해할 수 있는 정보 ※「개인정보 보호법」 제23조 및 동법 시행령 제18조
				인증정보	비밀번호, 바이오정보(지문, 홍채, 정맥 등) ※「개인정보의 안전성 확보조치 고시」 제2조
				신용정보/금융정보	신용정보, 신용카드번호, 계좌번호 등 ※「신용정보의 이용 및 보호에 관한 법률」 제2조, 제19조 및 동법 시행령 제2조, 제16조, 제21조, 별표2 등

등급	조합설명	위험성	자산가치	분류	개인정보 종류
				의료정보	건강상태, 진료기록 등 ※「의료법」 제22조, 제23조 및 동법 시행규칙 제14조 등
				위치정보	개인 위치정보 등 ※「위치정보의 보호 및 이용 등에 관한 법률」 제2조, 제16조 등
				기타 중요정보	해당 사업의 특성에 따라 별도 정의
2 등급	조합되면 명확히 개인의 식별이 가능한 개인정보	·정보주체의 신분과 신상정보에 대한 확인 또는 추정 가능 ·광범위한 분야에서 불법적인 이용 가능 ·유출 시 민/형사상 법적 책임 부여 가능 및 대외 신인도 저하	3	개인식별 정보	이름, 주소, 전화번호, 핸드폰번호, 이메일 주소, 생년월일, 성별 등
				개인관련 정보	학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등
				기타 중요 정보	개인 영상정보
3 등급	개인식별 정보와 조합되면 부가적인 정보를 제공하는 간접 개인정보	·정보주체의 활동 성향 등에 대한 추정 가능 ·제한적인 분야에서 불법적인 이용 가능 ·대외 신인도 다소 저하	1	자동생성 정보	IP정보, MAC주소, 사이트 방문기록, 쿠키(cookie) 등
				가공정보	통계성 정보, 가입자 성향 등
				제한적 본인식별 정보	회원정보, 사번, 내부용 개인식별정보 등
				기타간접 개인정보	해당 사업의 특성에 따라 별도 정의

[표30] 개인정보 영향도 등급표

- 개인정보 침해요인 발생가능성은 다음의 표와 같이 4가지로 구분하여 평가함

구분	발생 가능성	중요도
매우 높음	해당 침해요인의 발생 가능성이 높은 경우	3
높음	해당 침해요인의 발생 가능성이 그다지 높지 않은 경우	2
중간	해당 침해요인의 발생 가능성이 희박하다고 판단되는 경우	1
낮음	해당 침해요인의 발생 가능성이 없는 경우	0

[표31] 개인정보 침해요인 발생가능성 평가 기준

- 법적 준거성은 다음의 표와 같이 2가지로 구분하여 평가함

구분	발생 가능성	중요도
높음	법적 준수사항	1.5
낮음	법률 외 요건 (권장사항)	1

[표32] 법적 준거성 평가 기준

5.2 위험도 산정 결과

1) 대상기관 개인정보보호 관리체계

자산명	ABC공공기관 홈페이지 시스템	위험도	개인정보 영향도	발생 가능성	법적 준거성
처리단계	-				
질의문 코드	1.1.2	8	5	1	1.5
침해요인	개인정보보호책임자가 정보주체의 개인정보 보호를 위해 개인정보 보호법령에서 반드시 수행하도록 규정한 업무를 누락할 경우 관련 법령 조항을 준수하지 못하게 되며, 개인정보의 안전한 관리를 위한 조치가 미비될 위험이 있음				

[표33] 대상기관 개인정보보호 관리체계 위험도 산정결과

2) 대상시스템 개인정보보호 관리체계

자산명	ABC공공기관 홈페이지 시스템	위험도	개인정보 영향도	발생 가능성	법적 준거성
처리단계	-				
질의문 코드	2.1.1	8	5	1	1.5
침해요인	개인정보를 처리하는 개인정보취급자가 정보주체의 개인정보 보호를 위해 개인정보보호법령에서 반드시 수행하도록 규정한 업무를 누락할 경우 관련 법령 조항을 준수하지 못하게 되며, 개인정보의 안전한 관리를 위한 조치가 미비될 위험이 있음				

[표34] 대상시스템 개인정보보호 관리체계 위험도 산정결과

3) 개인정보처리단계별 보호조치

자산명	ABC공공기관 홈페이지 시스템	위험도	개인정보 영향도	발생 가능성	법적 준거성
처리단계	수집단계				
질의문 코드	3.1.1	12	3	3	1.5
침해요인	통합회원 가입 시 수집한 개인정보 이외의 항목을 추가로 수집할 경우 정보주체의 동의가 없다면 개인정보 보호법에서 규정한 수집근거 없이 무단으로 수집하게 되는 위험이 있음				

[표35] 개인정보처리단계별 보호 위험도 산정결과

5.3 개선방안 도출

- 영향평가 결과에 따라 위험을 도출하고, 해당 위험을 제거하기 위한 대상기관 개인정보보호 관리체계 관련 개선방안을 다음과 같이 자산(시스템)별로 구분하여 도출함.

가. 홈페이지 시스템

위험도	자산명	질의문 코드	침해요인	개선방안
12	홈페이지 시스템	3.1.1	통합회원 가입 시 수집한 개인정보 이외의 항목을 추가로 수집할 경우 정보주체의 동의가 없다면 개인정보 보호법에서 규정한 수집근거 없이 무단으로 수집하게 되는 위험이 있음	- 각 업무별 신청 접수 시 통합회원 가입 시 기 수집한 항목 이외에 추가로 수집하는 개인정보에 대하여 정보주체로부터 수집 동의 받을 수 있도록 개선

[표36] 침해요인별 개선방안 도출

나. 통합회원 관리 시스템

위험도	자산명	질의문 코드	침해요인	개선방안
11	통합회원 관리 시스템	2.1.1	모든 통합회원 정보를 조회하거나 변경할 수 있는 권한을 가진 취급자가 많아질수록 개인정보 무단이용 또는 유출 위험이 증가하게 되며, 개인정보 처리자의 관리 감독 범위가 확대되어 효과적인 통제가 어려워질 위험이 있음.	- 통합회원관리시스템 관리자 권한은 모든 통합회원의 모든 개인정보를 처리할 수 있으므로 권한보유자를 시스템관리자로 제한하거나 접근 권한 부여절차 수립에 따라 부서별 인원을 제한

[표37] 침해요인별 개선방안 도출

다. CCTV 시스템

위험도	자산명	질의문 코드	침해요인	개선방안
6	CCTV 시스템	5.1.1	CCTV 설치 운영 전 이해관계인의 의견을 수렴하는 절차를 거치지 않는다면 개인정보보호법령에서 정한 영상정보 설치 제한에 따른 조항을 준수하지 못하게 됨.	- CCTV를 설치할 경우에는 이해관계인(내부 근무자 및 ○○○ 이용자)을 대상으로 설명회를 개최하거나, 설문조사/여론조사 등을 통하여 의견을 수렴하는 절차를 거치도록 'ABC공공기관 CCTV 설치·운영 규정'을 개정

[표38] 침해요인별 개선방안 도출

5.4 개선계획 수립

- 영향평가 결과 개인정보 침해위험을 제거하기 위한 개선과제 이행이 필요하며, 위험평가 결과에 따라 개선과제의 수행시기를 제시함
- 개선방안을 기준으로 ABC공공기관 내 보안조치현황, 예산, 인력, 사업 일정 등을 고려하여 개인정보보호담당자 및 시스템담당자와 협의하여 아래와 같이 개선계획을 수립하였으며, 권장사항 중 현실적 여건 상 적용하기 어려운 과제는 제외하였음

1) 개선계획 수립

순번	개선과제	개선내용	담당부서	이행 구분	수행 시기	과제성격 (예산)
1	○○,○○,○○ 등 신청 접수 시 추가 수집 개인정보에 대한 수집동의 획득	- 각 업무별 신청 접수 시 통합회원 가입 시 기 수집한 항목 이외에 추가로 수집하는 개인정보에 대하여 정보주체로부터 수집 동의 받을 수 있도록 개선(3.1.1) - 각 업무별 신청 접수 시 추가로 수집하는 개인정보에 대하여 정보 주체에게 수집사실을 알리도록 개선(3.1.1)	각 업무 주관부서	필수	2020년 9월	시스템 수정
2	개인정보처리업무 수탁업체에 대한 개인정보보호현황 점검 절차 수립 및 이행	- 개인정보보호규정에 개인정보 처리 위탁 시 수탁자가 준수해야 할 책임사항을 규정하고 수탁기관과의 계약서에도 해당조항을 포함하도록 개선(3.4.2) - 개인정보처리업무를 위탁하는 경우 수탁자 책임사항 이행 여부 점검항목을 세분화하여 실질적인 점검이 가능하도록 보완(3.4.3)	보안팀	필수	2020년 12월	정책 제·개정
3	....	....	....	....	....	....

[표39] 개선계획서

2) 개선계획 상세 이행방안

<table>
<tr><td>개선 과제명</td><td>○○, ○○, ○○ 등 신청 접수 시 추가 수집 개인정보에 대한 수집동의 획득</td><td>순번</td><td>1</td></tr>
<tr><td>관련 평가항목</td><td>3.1.1</td><td>법적요건</td><td>법률근거</td></tr>
<tr><td>과제내용</td><td colspan="3">– 각 업무별 신청 접수 시 통합회원 가입 시 기 수집한 항목 이외에 추가로 수집하는 개인정보에 대하여 정보주체로부터 수집 동의 받을 수 있도록 개선(3.1.1)
– 각 업무별 신청 접수 시 추가로 수집하는 개인정보에 대하여 정보주체에게 수집사실을 알리도록 개선(3.1.1)
· 동의 받는 서식(○○○ 신청접수 인 경우) 예시

수집·이용하는 항목 : 성명, 학력, 경력, ○○내역(활동명, 기간, 기관명)
수집·이용목적 : 본인확인 및 본인에게 적합한 ○○ 배정
보유 및 이용기간 : 00년
상기 개인정보 수집 및 이용에 동의하지 않을 수 있으며, 동의하지 않을 경우 신청사항이 허가되지 않을 수 있습니다.

상기와 같이 개인정보 수집에 동의함 □ 동의 안함 □</td></tr>
<tr><td>담당부서</td><td>각 업무 주관부서</td><td>수행시기</td><td>2020년 9월</td></tr>
<tr><td>개선 과제명</td><td>개인정보처리업무 수탁업체에 대한 개인정보보호현황 점검 절차 수립 및 이행</td><td>순번</td><td>2</td></tr>
<tr><td>관련 평가항목</td><td>3.4.2, 3.4.3</td><td>법적요건</td><td>법률근거</td></tr>
<tr><td>과제내용</td><td colspan="3">– 개인정보보호규정에 개인정보 처리 위탁 시 수탁자가 준수해야 할 책임사항을 규정하고 수탁기관과의 계약서에도 해당조항을 포함하도록 개선(3.4. 2)
· 위탁계약서에 반드시 포함해야 할 항목

● 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
● 개인정보의 기술적 · 관리적 보호조치에 관한 사항
● 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항
· 위탁업무의 목적 및 범위
· 재위탁 제한에 관한 사항
· 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
· 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
· 수탁자 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

– 개인정보처리업무를 위탁하는 경우 수탁자 책임사항 이행 여부 점검항목을 세분화하여 실질적인 점검이 가능하도록 보완(3.4.3)
· 수탁자의 개인정보보호 관리실태 점검을 년 1회 이상 실시하거나, 수탁자가 자체적으로 실시한 결과를 보고하도록 위탁계약서에 명시
· 체크 항목은 ABC공공기관이 OOOO년 O월에 자체적으로 실시한 “개인정보보호 필수조치사항 자체점검” 시 사용한 체크리스트 참조</td></tr>
<tr><td>담당부서</td><td>시스템운영과</td><td>수행시기</td><td>2020년 12월</td></tr>
</table>

6. 총평

영향평가 대상사업인 ABC공공기관 홈페이지 시스템의 개인정보 침해 위험성을 대상기관의 개인정보보호 관리체계, 대상 시스템의 개인정보보호 관리체계 및 대상 시스템의 개인정보 생명주기별 보호조치를 분석·평가하였음

ABC공공기관의 개인정보보호 관리체계에 대한 점검 결과, 개인정보처리방침을 통한 안내, 정보주체의 권익보호 및 개인정보처리구역 보호 등은 양호한 것으로 평가함. 그러나 내부 관리계획과 개인정보파일대장 관리절차, 개인정보 침해, 유출사고 대응체계 수립 등이 미흡한 것으로 평가함

홈페이지 시스템의 관리체계에 대한 점검 결과, 개인정보 취급내용에 대한 안내는 양호한 것으로 평가함. 하지만 개인정보 취급자 지정이 관련 법령에서 요구하는 사항을 충족하지 못하는 것으로 평가함

홈페이지 시스템의 생명주기별 보호조치에 대한 점검 결과, 회원가입 이후에 추가 수집하는 개인정보에 대한 정보주체의 동의가 누락되어 있어 개선이 필요하며 보유기간 경과 후에도 개인정보가 파기되지 않는 문제점이 발견됨

홈페이지 시스템 기술적 보호조치 영역은 외국인 등록번호(또는 여권번호) 입력 화면에 대한 마스킹 처리 미비, 비밀번호 일방향 암호화 저장 미적용 등 다수 점검항목에 대해 개선해야 할 사항으로 도출되었음

도출된 침해요인은 대부분 단기적으로 조치 가능한 사항이 많으므로, 개선계획을 충실히 이행함으로써 개인정보 침해 위험을 최소화하도록 관리가 필요함

개인정보 영향평가 항목
(요약)

평가영역	평가분야	세부분야	No.	평가항목
1. 대상기관 개인정보 보호 관리체계	1.1 개인정보 보호 조직	개인정보보호 책임자의 지정	1.1.1	개인정보 보호책임자를 법령기준에 따라 지정하고 있습니까?
		개인정보보호 책임자 역할수행	1.1.2	개인정보 보호책임자에게 법령 등이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?
	1.2 개인정보 보호 계획	내부 관리계획 수립	1.2.1	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있습니까?
			1.2.2	개인정보보호책임자는 연1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 있습니까?
		개인정보보호 연간 계획 수립	1.2.3	개인정보보호 교육, 실태점검 등 개인정보보호 활동에 대한 연간 수행계획을 수립·시행하고 있습니까?
	1.3 개인정보 침해대응	침해사고 신고방법 안내	1.3.1	개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?
		유출사고 대응	1.3.2	개인정보 유출 신고·통지 절차, 긴급 연락체계, 사고대응 조직 구성 등을 포함한 개인정보 침해사고 대응 절차를 수립하여 실시하고 있습니까?
	1.4 정보주체 권리보장	정보주체 권리보장 절차 수립	1.4.1	개인정보 열람, 정정·삭제, 처리정지, 수집출처 고지 등 정보주체의 요구에 대한 처리절차를 수립하여 실시하고 있습니까?
		정보주체 권리보장 방법 안내	1.4.2	정보주체의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하고 있습니까?
2. 대상시스템의 개인정보 보호 관리체계	2.1 개인정보 취급자 관리	개인정보 취급자 지정	2.1.1	업무상 필요한 최소한의 범위로 최소한의 인원이 개인정보를 처리하도록 개인정보취급자를 지정하도록 계획하고 있습니까?
		개인정보취급자 관리·감독	2.1.2	개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호서약서 작성 등 관리·감독을 계획하고 있습니까?
	2.2 개인정보 파일 관리	개인정보파일 대장 관리	2.2.1	대상시스템에서 개인정보파일을 신규로 보유하거나 변경하는 경우, 개인정보파일대장을 작성하거나 변경하도록 계획하고 있습니까?
		개인정보파일 등록	2.2.2	대상시스템에서 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우, 개인정보보호위원회에 등록하도록 계획하고 있습니까?
	2.3 개인정보 처리방침	개인정보 처리방침의 공개	2.3.1	개인정보 처리방침을 수립하고 인터넷 홈페이지·관보 등에 안내하도록 계획하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
		개인정보 처리방침의 작성	2.3.2	개인정보 처리방침은 법률 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?
3. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성	3.1.1	개인정보를 수집하는 경우 법령에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?
			3.1.2	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고 있습니까?
			3.1.3	주민등록번호는 법적 근거가 있는 경우에 한하여 수집하고 있으며, 인터넷 홈페이지에 대해서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고 있습니까?
		동의받는 방법의 적절성	3.1.4	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있습니까?
			3.1.5	만14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받도록 계획하고 있습니까?
			3.1.6	개인정보 관련 동의를 서면으로 받을 때에는 중요한 내용을 명확히 표시하여 알아보기 쉽게 하고, 개인정보 수집·이용, 제3자 제공, 목적외 이용 등에 대해 각각 구분하여 동의를 받도록 계획하고 있습니까?
			3.1.7	민감정보, 고유식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의를 받도록 계획하고 있습니까?
	3.2 보유	보유기간 산정	3.2.1	개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정하도록 계획하고 있습니까?
	3.3 이용·제공	개인정보 제공의 적합성	3.3.1	개인정보를 제3자에게 제공하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?
			3.3.2	개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?
		목적 외 이용·제공 제한	3.3.3	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 별도의 동의를 받거나 관련 법률에 근거하도록 계획하고 있습니까?
			3.3.4	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 이용목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?
			3.3.5	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 '개인정보 목적 외 이용 및 제3자 제공 대장'에 기록·관리하도록 계획하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
			3.3.6	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 관련 내용을 관보 또는 인터넷 홈페이지 등을 통해 공개하도록 계획하고 있습니까?
		제공시 안전성 확보	3.3.7	개인정보를 제3자에게 제공하거나 연계하는 경우 암호화 조치, 보유기간 지정 등 안전성 확보를 위해 필요한 조치를 적용하도록 계획하고 있습니까?
	3.4 위탁	위탁사실 공개	3.4.1	개인정보 처리에 관한 업무 위탁시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하도록 계획하고 있습니까?
		위탁 계약	3.4.2	개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?
		수탁사 관리·감독	3.4.3	개인정보 처리에 관한 업무를 위탁받아 처리하는 자(수탁자)를 대상으로 개인정보보호 교육, 처리현황 점검 등 관리·감독 활동을 계획하고 있습니까?
	3.5 파기	파기 계획 수립	3.5.1	개인정보의 보유 목적이 달성되었거나 보유 기간이 경과되었을 때 지체없이 파기되도록 계획하고 있습니까?
		분리보관 계획 수립	3.5.2	다른 법령 등에 따라 개인정보를 보존할 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하도록 계획하고 있습니까?
		파기대장 작성	3.5.3	개인정보파일을 파기하는 경우 파기 결과 등을 '개인정보파일 파기 관리대장'에 기록·관리하도록 계획하고 있습니까?
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	계정 관리	4.1.1	개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하도록 계획하고 있습니까?
		인증 관리	4.1.2	개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?
			4.1.3	정보주체가 비밀번호 변경 등 중요 정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용되도록 계획하고 있습니까?
			4.1.4	대량의 개인정보 또는 중요한 개인정보를 처리하는 개인정보취급자 및 관리자는 강화된 인증방식이 적용되도록 계획하고 있습니까?
			4.1.5	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
			4.1.6	개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 계획하고 있습니까?
			4.1.7	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 장기 미접속시 계정 잠금, 동시 접속 제한, 관리자 로그인 알림 등 보호 대책이 적용되도록 계획하고 있습니까?
		권한 관리	4.1.8	개인정보취급자가 변경될 경우 지체없이 개인정보처리 시스템의 접근권한을 변경 또는 말소하도록 계획하고 있습니까?
			4.1.9	개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 기록하도록 계획하고 있습니까?
			4.1.10	개인정보처리시스템에 대한 개인정보취급자의 권한을 조회, 입력, 변경, 삭제, 출력, 다운로드 등 그 역할에 따라 최소한으로 부여할 수 있도록 계획하고 있습니까?
	4.2 접근통제	접근통제 조치	4.2.1	개인정보처리시스템에 대한 불법적인 접근 및 침해 사고를 방지할 수 있도록 접근통제시스템을 설치·운영 하도록 계획하고 있습니까?
			4.2.2	개인정보취급자가 정보통신망을 통해 외부에서 개인 정보처리시스템에 접속하려는 경우에는 가상사설망 (VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하도록 계획하고 있습니까?
			4.2.3	인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인 정보처리시스템, 개인정보취급자 PC, 모바일기기 등에 보호조치를 계획하고 있습니까?
			4.2.4	개인정보처리자는 개인정보 유출 등 개인정보 침해 사고 방지를 위하여 관리용 단말기에 대한 안전 조치를 적용하도록 계획하고 있습니까?
		인터넷 홈페이지 보호조치	4.2.5	인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용 프로그램에 대한 취약점점검 및 대응조치를 수행하도록 계획하고 있습니까?
		업무용 모바일 기기 보호조치	4.2.6	개인정보를 처리하는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?
	4.3 개인정보의 암호화	저장시 암호화	4.3.1	고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
			4.3.2	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하도록 계획하고 있습니까?
		전송시 암호화	4.3.3	고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?
	4.4 접속기록의 보관 및 점검	접속기록 보관	4.4.1	개인정보처리시스템의 접속기록을 식별자, 접속 일시, 접속자를 알 수 있는 정보, 수행업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?
		접속기록 점검	4.4.2	개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 정기적으로 점검하도록 계획하고 있습니까?
		접속기록 보관 및 백업	4.4.3	개인정보처리시스템의 접속기록을 최소 2년 이상 보관하고 위·변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관하도록 계획하고 있습니까?
	4.5 악성 프로그램 등 방지	백신 설치 및 운영	4.5.1	개인정보처리단말기에 악성프로그램을 점검, 치료할 수 있는 백신프로그램을 설치하고 최신업데이트 및 악성프로그램의 주기적 점검 등 대응조치를 실시하도록 계획하고 있습니까?
		보안업데이트 적용	4.5.2	악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램, 운영체제 소프트웨어 제작업체에서 보안 업데이트 공지가 있는 경우, 이에 따른 업데이트가 지체 없이 실시되도록 계획하고 있습니까?
	4.6 물리적 접근 방지	출입통제 절차 수립	4.6.1	전산실, 자료보관실 등 개인정보를 보관하는 물리적 장소에 대한 출입통제 절차를 수립·운영하도록 계획하고 있습니까?
		반출·입 통제절차 수립	4.6.2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하도록 계획하고 있습니까?
	4.7 개인정보의 파기	안전한 파기	4.7.1	개인정보를 파기할 경우 복구 또는 재생되지 않는 방법으로 파기하도록 계획하고 있습니까?
	4.8 기타 기술적 보호조치	개발환경 통제	4.8.1	개발환경을 통한 개인정보의 유출을 방지하기 위하여 테스트 데이터 생성, 이용, 파기 및 기술적 보호조치 등에 관한 대책을 적용하도록 계획하고 있습니까?
		개인정보 처리화면 보안	4.8.2	개인정보취급자 및 정보주체의 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 카드번호 등 중요 정보에 대한 복사·화면 캡쳐 방지 및 키보드해킹 방지 등 보호대책을 적용하도록 계획하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
		출력 시 보호조치	4.8.3	개인정보취급자가 개인정보를 종이로 출력할 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책을 적용하도록 계획하고 있습니까?
	4.9 개인정보 처리구역 보호조치	보호구역 지정	4.9.1	개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 CCTV, 출입통제 장치, 화재 경보기 등 보호설비를 설치·운영하도록 계획하고 있습니까?
			4.9.2	개인정보처리자는 화재, 홍수, 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검하도록 계획하고 있습니까?
			4.9.3	개인정보처리자는 재해 · 재난 발생 시 개인정보처리 시스템 백업 및 복구를 위한 계획을 마련하도록 계획하고 있습니까?
5. 특정IT 기술 활용 시 개인정보 보호	5.1 CCTV	CCTV 설치 시 의견수렴	5.1.1	CCTV 설치시 관계 전문가 및 이해관계인의 의견을 수렴하도록 계획하고 있습니까?
		CCTV 설치 안내	5.1.2	CCTV 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나 홈페이지, 이메일 등을 통해 안내하도록 계획하고 있습니까?
		CCTV 사용 제한	5.1.3	CCTV 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 계획하고 있습니까?
			5.1.4	CCTV 운영 시 CCTV에 대한 운영·관리방침을 수립하도록 계획하고 있습니까?
		CCTV 설치 및 관리에 대한 위탁	5.1.5	CCTV 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 계획하고 있습니까?
	5.2 RFID	RFID 이용자 안내	5.2.1	RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하도록 계획하고 있습니까?
			5.2.2	RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기하도록 계획하고 있습니까?
			5.2.3	RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻도록 계획하고 있습니까?
			5.2.4	RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하도록 계획하고 있습니까?

평가영역	평가분야	세부분야	No.	평가항목
		RFID 태그 부착 및 제거	5.2.5	구입 및 제공받은 물품에 RFID 태그가 내장 및 부착 되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하도록 계획하고 있습니까
			5.2.6	RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 계획하고 있습니까?
			5.2.7	이용자의 신체에 RFID를 지속적으로 착용하지 않도록 계획하고 있습니까?
	5.3 바이오정보	원본정보 보관시 보호조치	5.3.1	수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?
			5.3.2	원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 계획하고 있습니까?
	5.4 위치정보	개인위치정보 수집 동의	5.4.1	개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?
		개인위치정보 제공시 안내사항	5.4.2	개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하도록 계획하고 있습니까?

개인정보 영향평가 항목
(평가표)

1. 대상기관 개인정보보호 관리체계

1 개인정보보호 조직

세부분야	개인정보 보호책임자의 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.1.1	● **개인정보 보호책임자를 법령기준에 따라 지정하고 있습니까?**		○		
평가 예시	● 이행 : 개인정보 보호책임자를 지정 기준에 따라 지정하고, 지침 또는 직무기술서, 임명장 등 관련 문서 등을 통해 개인정보 보호책임자의 지정사실을 알리고 있는 경우 ● 부분 이행 : 개인정보 보호책임자가 지정되어 있으나 지정기준을 만족하지 못하거나, 지정사실을 전체 직원이 알 수 있도록 공식화하지 않은 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 4급 이상의 공무원 자격 기준을 만족하고 있는 자를 개인정보 보호책임자로 지정하여야 하나, 현재 5급 공무원이 책임자로 지정되어 있음				

주요 점검 사항

1. 개인정보 보호책임자는 인사발령 등을 통해 공식적으로 지정되어야 한다.
2. 개인정보 보호책임자는 개인정보 처리에 관한 업무를 총괄하여 책임질 수 있도록 법적 요건을 충족하는 자로 지정되어야 한다.

지표 해설

- 개인정보 보호책임자는 개인정보 법규 준수, 유출 및 오남용 방지 등 개인정보 처리자의 개인정보보호 활동을 촉진하기 위한 자주적 규제 장치의 하나라고 할 수 있다. 조직 내에서 개인정보 처리에 관한 업무를 총괄하여 책임질 임원 내지 부서장급의 책임자를 지정·운영함으로써 개인정보처리자의 내부 관리체계를 더욱 공고히 할 수 있다.

- 개인정보 보호책임자는 개인정보 처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대하여 책임을 지는 자이므로 개인정보 수집·이용·제공 등에 대하여 실질적인 권한을 가지고 있어야 하며 조직 내에서 어느 정도 독자적인 의사결정을 할 수 있는 지위에 있는 자이어야 한다.

- 개인정보처리자는 개인정보 법규 준수, 유출 및 오·남용 방지 등 개인정보처리자의 개인정보보호 활동을 촉진하기 위하여 법적 지정 기준에 따른 개인정보 보호책임자를 지정하여야 한다.

공공기관 개인정보 보호책임자 자격 요건		
공공기관		자격요건
①	국회, 법원, 헌법재판소, 중앙선관위, 중앙행정기관	고위공무원단
②	① 외의 정무직공무원을 장으로 하는 국가기관	3급 이상 공무원
③	①, ② 외의 고위3급 공무원을 장으로 하는 국가기관	4급 이상 공무원
④	①~③ 외의 국가기관	개인정보처리업무담당 부서장
⑤	시 · 도 및 시 · 도 교육청	3급 이상 공무원
⑥	시 · 군 및 자치구	4급 이상 공무원
⑦	각급 학교	행정사무를 총괄하는 자
⑧	①~⑦ 외의 공공기관	개인정보처리업무담당 부서장

- 민간사업자는 대표자, 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 소양이 있는 사람을 개인정보 보호책임자로 지정하여야 한다.
- 개인정보 보호책임자를 지정·변경한 경우 모든 직원들이 알 수 있도록 지침, 임명장, 인사발령 등의 절차를 통해 지정사실을 공식화하여야 하며, 또한 개인정보처리방침 내 책임자의 지정 및 변경사실 등을 공개하여야 한다.

용어설명

※ 개인정보 보호책임자 : 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 「개인정보 보호법」 제31조와 시행령 제32조에 따른 지위에 해당하는 자를 말한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.1.1	개인정보 보호책임자를 법령기준에 따라 지정하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 인사발령을 통하여 ○○국장을 개인정보 보호책임자로 지정하였고 홈페이지의 개인정보 처리방침에 안내하고 있음. 하지만 △△△ 기관은 4급 이상을 개인정보보호책임자로 지정해야 하나 ○○ 국장은 사무관(5급)으로 지정기준을 만족하지 못함.				

개인정보보호 책임자 인사발령	1. 개인정보보호 책임자 인사발령 1 XX국 XX국장 [redacted] ○○국장 [redacted]
개인정보보호 책임자 공개	제23조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.
업무분장표	○○○국 업무분장표 2013. 11. 2.현재 분야 / 급수 / 직렬(직급) / 성명 / 담당업무 총괄 / 5급 / 국장(사무관) / ○○ / 개인정보보호책임자 ○○국 업무 총괄 / / 7급 / 행정주사보 / ○○ / ○과 서무 업무 ○법령 결의회신 및 타기관 법령 의견 조회 ○국회 및 예·결산 총괄

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제31조(개인정보 보호책임자의 지정)

① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

【개인정보 보호법 시행령】

제32조(개인정보 보호책임자의 업무 및 지정요건 등)

② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.

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. 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제31조

세부분야	개인정보 보호책임자 역할 수행				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.1.2	● **개인정보 보호책임자에게 법령 등이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?**		○		
평가 예시	● 부분 이행 : 개인정보 보호책임자의 업무가 문서로 정의되어 있으나 법률에서 요구하는 요건 중 일부만을 반영하거나, 업무는 수행하고 있으나 문서로 증명할 수 없는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '개인정보보호지침'에 개인정보보호법 제31조에 준하여 개인정보 보호책임자의 업무를 부여하고 있으나 법령에서 부여하고 있는 업무에 대하여 실질적으로 수행하고 있지 않음				

주요 점검 사항

1. 개인정보 보호책임자에게 법률 등에서 정하는 책임 및 역할이 공식적으로 부여되어야 한다.
2. 개인정보 보호책임자는 개인정보 보호계획의 수립·시행, 개인정보처리 실태 및 관행의 조사·개선 등 관련 업무를 실제로 수행하여야 한다.

지표 해설

- 개인정보 보호책임자의 업무는 총괄책임자로서 지는 업무이므로, 개인정보 보호책임자는 분야별로 개인정보 보호관리자, 개인정보 보호담당자 등을 두어 업무를 하게 할 수 있다.

개인정보 보호책임자의 역할
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. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 8. 개인정보 보호 관련 자료의 관리 9. 처리목적이 달성되거나 보유기간이 경과한 개인정보의 파기

- 개인정보 보호책임자의 책임 및 역할은 내부 관리계획, 개인정보보호지침 등 문서로 정의되어 승인되어야 한다.
- 개인정보 보호책임자는 법령 등에서 부여한 책임 및 역할을 실질적으로 수행하여야 하며, 내부관리체계 강화를 위하여 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받아야 한다. 또한 법령 등 위반사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요 시 해당 기관장에게 개선조치를 보고하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.1.2	개인정보 보호책임자에게 법령 등이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 '개인정보보호지침'에 개인정보 보호책임자의 업무 및 역할을 명시하였으나, 법령에서 요구하는 사항 일부(개인정보 보호 관련 자료의 관리, 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기)가 누락됨				

개인정보 보호지침	**제5조(개인정보보호 책임자)** ① 개인정보보호 책임자는 병원의 기획조정실장으로 하며, 병원의 개인정보보호 및 보안에 관한 업무를 총괄하여 수행한다. ② 개인정보보호 책임자는 다음 각 호의 업무를 수행한다. 1. 개인정보보호 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. 개인정보보호 교육 계획의 수립 및 시행 6. 개인정보파일의 보호 및 관리감독 7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 8. 개인정보보호 관련 자료의 관리 9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 10. 그 밖에 개인정보보호 및 보안과 관련한 주요 사항

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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(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

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제31조

2 개인정보 보호계획

세부분야	개인정보보호 계획				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.2.1	● **개인정보의 안전한 처리를 위한 내부관리 계획을 수립·시행하고 있습니까?**		○		
평가 예시	● 부분이행 : 내부 관리계획을 수립하고 있으나, 내부 결재를 거치지 않았거나 반드시 포함되어야 할 내용이 일부 누락되어 있는 경우				
평가근거 및 의견	● △△△기관은 『개인정보의 안전성 확보조치 기준』에 따라 유형3에 속하는 공공기관으로 2020년 내부 관리계획이 수립되어 있으나, 내부 관리계획서 내에 개인정보 처리업무 수탁자에 대한 관리 및 감독에 관한 사항이 빠져 있음				

주요 점검 사항

1. 내부 관리계획을 수립하고 내부 의사결정 절차를 통해 공식적으로 시행하여야 한다.

2. 내부 관리계획에는「개인정보의 안전성 확보조치 기준」에 명시된 모든 내용이 포함되어야 한다. (유형1, 유형2, 유형3에 따른 내용이 다르므로 구분하여 평가하여야 함)

① 개인정보 보호책임자 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 등

3. 개인정보 보호책임자 변경, 개인정보 보호법 개정 등 내부 관리계획 관련 사항에 중요한 변경이 있는 경우, 이를 반영하여 수정·시행하고 그 수정이력을 관리하여야 한다.

4. 내부 관리계획은 이해관계자에게 배포되고 공유되어야 한다.

지표 해설

- 개인정보처리자는 개인정보의 안전한 처리를 위하여 '내부 관리계획'을 수립하고 내부 의사결정 절차를 통하여 공식적으로 수립·시행하여야 한다.
- 내부 관리계획은「개인정보의 안전성 확보조치 기준」고시 제4조 제1항에서 명시된 사항을 모두 포함하여야 한다. (유형1은 내부 관리계획을 수립하지 않을 수 있음)

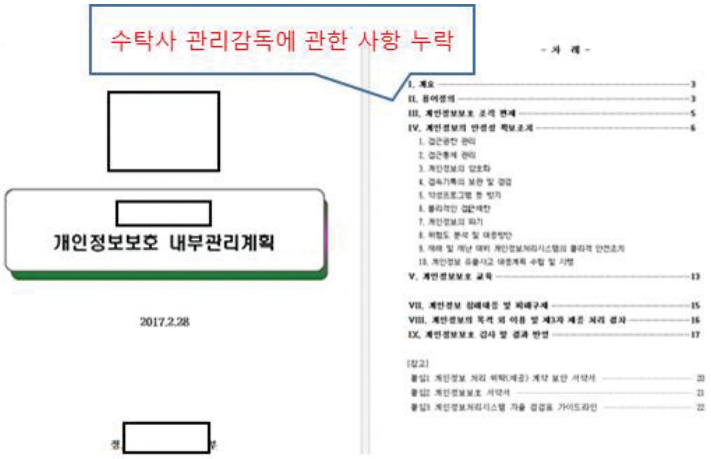
내부 관리계획에 포함되어야 하는 사항			
번호	내용	유형2	유형3
1	개인정보 보호책임자의 지정에 관한 사항	●	●
2	개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	●	●
3	개인정보취급자에 대한 교육에 관한 사항	●	●
4	접근 권한의 관리에 관한 사항	●	●
5	접근 통제에 관한 사항	●	●
6	개인정보의 암호화 조치에 관한 사항	●	●
7	접속기록 보관 및 점검에 관한 사항	●	●
8	악성프로그램 등 방지에 관한 사항	●	●
9	물리적 안전조치에 관한 사항	●	●
10	개인정보 보호조직에 관한 구성 및 운영에 관한 사항	●	●
11	개인정보 유출사고 대응 계획 수립·시행에 관한 사항	●	●
12	위험도 분석 및 대응방안 마련에 관한 사항	●	●
13	재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항		●
14	개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항		●
15	그 밖에 개인정보 보호를 위하여 필요한 사항	●	●

- 개인정보 보호법 개정, 개인정보 보호책임자 변경, 개인정보보호 교육 계획의 변경 등 내부 관리계획에 포함된 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.
- 내부 관리계획은 개인정보취급자 등 관련자들이 내용을 인지하고 준수할 수 있도록 공유되고 교육되어야 한다.
- 내부 관리계획의 문서 제목은 가급적 "내부 관리계획"이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 상황에 따라 다른 용어를 사용할 수 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.2.1	개인정보의 안전한 처리를 위한 내부관리 계획을 수립·시행하고 있습니까?		○		
평가근거 및 의견	● △△△기관은 『개인정보의 안전성 확보조치 기준』에 따라 유형3에 속하는 공공기관으로 2020년 내부 관리계획이 수립되어 있으나, 내부 관리계획서 내에 개인정보 처리업무 수탁자에 대한 관리 및 감독에 관한 사항이 빠져 있음				

번호	내용	적용여부
1	개인정보 보호책임자의 지정에 관한 사항	"III. 개인정보보호 조직 편제"에 작성되어 있음
2	개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	"III. 개인정보보호 조직 편제"에 작성되어 있음
3	개인정보취급자에 대한 교육에 관한 사항	"V. 개인정보보호 교육"에 작성되어 있음
4	접근 권한의 관리에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 1. 접근권한 관리 부분에 작성되어 있음
5	접근 통제에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 2. 접근통제 관리 부분에 작성되어 있음
6	개인정보의 암호화 조치에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 3. 개인정보의 암호화 부분에 작성되어 있음
7	접속기록 보관 및 점검에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 4. 접속기록의 보관 및 점검 부분에 작성되어 있음
8	악성프로그램 등 방지에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 5. 악성프로그램 등 방지 부분에 작성되어 있음
9	물리적 안전조치에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 6. 물리적인 접근제한 부분에 작성되어 있음
10	개인정보 보호조직에 관한 구성 및 운영에 관한 사항	"III. 개인정보보호 조직 편제"에 작성되어 있음
11	개인정보 유출사고 대응 계획 수립·시행에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 10. 개인정보 유출사고 대응계획 및 시행 부분에 작성되어 있음
12	위험도 분석 및 대응방안 마련에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 8. 위험도분석 및 대응방안 부분에 작성되어 있음
13	재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항	"VI. 개인정보의 안전성 확보조치"의 9. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치 부분에 작성되어 있음
14	개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항	누락되어 있음
15	그 밖에 개인정보 보호를 위하여 필요한 사항	"VII. 개인정보 침해대응 및 피해구제", 부분을 반영하고 있음



관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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

【개인정보 보호법 시행령】

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

【개인정보의 안전성 확보조치 기준】

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근권한의 관리에 관한 사항

5. 접근통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보보호를 위하여 필요한 사항

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조
- 개인정보의 안전성 확보조치 기준 해설서 – 제2장 제4조(내부 관리계획의 수립·시행)

세부분야	개인정보보호 계획				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.2.2	● **개인정보보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 있습니까?**			○	
평가 예시	● 미이행 : 내부 관리계획을 수립하고 있으나, 내부 관리계획에 대한 이행 실태를 점검하지 않는 경우				
평가근거 및 의견	● △△△기관은 『개인정보의 안전성 확보조치 기준』에 따라 유형3에 속하는 공공기관으로 2020년 내부 관리계획이 수립되어 있으나, 내부 관리계획에 대한 개인정보취급자들의 이행 실태를 점검하고 있지 않음				

주요 점검 사항

1. 개인정보 보호책임자는 내부 관리계획의 이행 실태를 연 1회 이상 점검하여야 한다.
2. 내부 관리계획 이행실태 점검후 문제점이 발견된 경우 이에 대한 조치계획을 수립하여 이행하여야 한다.

지표 해설

- 개인정보보호책임자는 내부 관리계획에 명시된 사항들이 제대로 준수되고 있는지에 대해 연 1회 이상 이행 실태를 점검하여야 한다.
- 이행실태 점검은 조직 내부에서 직접 수행하거나 외부 전문가를 활용할 수 있으며, 대상기관의 개인정보 처리 업무 환경 전반에 대하여 내부 관리계획의 이행실태가 충실히 점검될 수 있도록 점검계획을 수립·이행할 필요가 있다.
- 내부 관리계획 이행실태 점검결과는 개인정보 보호책임자에게 보고되어야 하며, 문제점으로 발견된 사항에 대해서는 조치계획을 수립하여 지속적으로 관리하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.2.2	개인정보보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 있습니까?			○	
평가근거 및 의견	● △△△기관은 『개인정보의 안전성 확보조치 기준』에 따라 유형3에 속하는 공공기관으로 2020년 내부 관리계획이 수립되어 있으나, 내부 관리계획에 대한 개인정보취급자들의 이행 실태를 점검하고 있지 않음				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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

【개인정보 보호법 시행령】

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

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

【개인정보의 안전성 확보조치 기준】

제4조(내부 관리계획의 수립·시행)

④ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조
- 개인정보의 안전성 확보조치 기준 해설서 – 제2장 제4조(내부 관리계획의 수립·시행)

세부분야	개인정보보호 계획				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.2.3	● **개인정보보호 교육, 실태 점검 등 개인정보 보호 활동에 대한 연간 수행계획을 수립·시행하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보보호 연간 계획 내에 개인정보 보호 교육계획만 수립되어 있고, 그 외 개인정보보호 활동을 위한 계획은 수립되지 않은 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '20XX년 개인정보보호 추진계획'의 '3.1 개인정보보호 교육 실시' 항목에 개인정보보호교육 계획만 수립하였고, 그 외 개인정보보호 활동을 위한 수탁사 관리감독 계획, 개인정보 파기 계획 등에 대한 계획은 수립되어 있지 않음				

주요 점검 사항

1. 개인정보보호 연간 계획이 수립되어, 내부 승인절차에 따라 시행되어야 한다.
2. 개인정보보호 연간 계획에는 아래와 같은 사항이 모두 포함되어야 한다.
   ① 개인정보보호 조직, 인력
   ② 개인정보보호 활동 계획 및 이에 따른 예산
   ③ 개인정보보호 실태 점검 계획(수탁자 포함)
   ④ 개인정보보호 교육 계획(책임자, 담당자, 취급자/일반직원 대상) 등
   ※ 실질적인 실행이 가능하도록 일정, 담당자, 예산 등 구체적인 방안 포함 필요
3. 개인정보 연간 계획에 따라 개인정보보호 활동이 이행되고 있는지 여부에 대해 정기적으로 검토하여 개인정보 보호 책임자에게 보고하여야 한다.

지표 해설

- 개인정보처리자는 취급하는 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성을 확보하기 위하여 개인정보 보호활동에 대한 조직 내부의 개인정보보호 연간 계획을 수립하고, 개인정보 처리와 관련된 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.
- 개인정보 보호계획을 수립하는 이유는 개인정보 보호활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하기 위함이다.
- 개인정보보호 연간계획은 개인정보처리자가 개인정보보호 활동을 체계적으로 하기 위해 필요한 사항이 모두 포함되어 있어야 한다.

개인정보보호 연간계획에 포함되어야 할 사항
1. 개인정보보호 조직, 인력 2. 개인정보보호 활동 계획 및 이에 따른 예산 3. 개인정보보호 실태 점검 계획(수탁자 포함) 4. 개인정보보호 교육 계획(책임자, 담당자, 취급자/일반직원 대상) 등

- 개인정보보호 연간 계획의 실행력을 확보하기 위해서는 사전에 수행 인력 및 예산이 확보되어야 하여, 연간 계획에 따라 활동이 수행되는지 정기적으로 검토 및 보고하여야 한다.
- 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 하며, 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 교육 내용도 각기 다를 수 있도록 상세 교육절차를 수립하여야 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.
- 교육은 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으며, 연간 교육계획을 수립하여 모든 개인정보취급자가 일정 시간 이상 교육에 참여할 수 있도록 하여야 한다.
- 교육은 매년 정기적으로 실시할 수 있도록 하며, 교육 수행 결과를 기록하고 다음 교육에 반영할 수 있도록 절차를 수립할 것을 권장한다.
- 개인정보처리자는 개인정보 보호책임자 및 개인정보취급자를 대상으로 매년 정기적으로 개인정보보호 교육을 실시하여야 한다. 특히, 개인정보취급자가 고객의 개인정보를 훼손·침해·누설할 경우에는 중벌에 처해지므로, 교육 시 이러한 점을 개인정보취급자에게 인식시키기 위해 노력해야 한다.
- 개인정보보호 교육의 구체적인 사항에는 교육을 하는 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하여야 하며, 내부 결재를 얻은 "○○○○년 개인정보보호 교육 계획(안)"과 같은 문서를 통해 관리하여야 한다.

개인정보보호 교육 내용(예시)
● 개인정보보호의 중요성 설명 ● 내부 관리계획의 준수 및 이행 ● 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략 ● 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법 ● 개인정보의 기술적·관리적 보호조치 기준 이행 ● 개인정보보호 위반을 보고해야 할 필요성 ● 개인정보보호업무의 절차, 책임, 작업 설명 ● 개인정보보호 관련자들의 금지 항목들 ● 개인정보보호 준수사항 이행 관련 절차 등

- 개인정보보호 활동은 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 장기적인 관점에서 개인정보보호 마스터플랜을 수립하고, 매년 1년 단위의 계획을 수립할 것을 권장한다.
- 본 지표는 법적 필수 사항은 아니며, 대상 기관의 체계적이고 지속적인 보안 관리를 위하여 준수가 필요한 권장사항이다.

  – 개인정보 교육계획이 내부 관리계획에 포함되어 있는지 여부는 지표 1.2.1에서 점검

  ※ 즉, 개인정보보호 교육과 관련하여 「개인정보 보호법」 및 「개인정보의 안전성 확보조치 기준 고시」에 따른 최소한의 필수 요건은 다른 지표(1.2.1, 2.1.2)에서 점검을 수행하고, 본 지표에서는 교육 계획의 구체성, 실효성 측면에서 점검 수행

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.2.3	개인정보보호 교육, 실태점검 등 개인정보보호 활동에 대한 연간 수행 계획을 수립·시행하고 있습니까?		○		

평가근거 및 의견

● △△△ 기관은 '20XX년 개인정보보호 추진계획'의 3.1.라 개인정보보호 교육 실시 항목에 개인정보보호 교육 계획을 수립(기본교육, 실무교육, 전문교육으로 구분하고, 목적, 대상, 횟수, 교육방법, 교육내용을 제시)하였고, '2월 개인정보 보호법 교육 결과보고(시행문)' 문서를 확인한 바, 계획에 따라 교육을 시행하고 있으나, 그 외 개인정보보호 활동을 위한 수탁사 관리감독 계획, 개인정보 파기 계획 등에 대한 계획은 수립되어 있지 않음.

20XX년 개인정보 보호 추진계획	**라. 개인정보보호 교육 실시** ○ 해당부서(기관) : 정보시스템팀, 전부서(기관) ○ 기본교육 - 목적 : 개인정보 보호의식 고취 및 침해사고 발생시 대응방법 등 - 대상 : 전직원 - 횟수 : 반기 1회 - 교육방법 : 기관(부서)별 자체교육 실시 - 교육내용 • 개인정보보호 관련 법령 이해 • 개인정보 침해 위협요인 및 사례 등 • 사업추진시 개인정보보호 확인사항 등 ○ 실무교육 - 목적 : 개인정보보호 실무지식 습득 - 대상 : 개인정보보호책임자 및 보호담당자 - 횟수 : 1회 - 방법 : 집합교육(정보시스템팀 주관) - 교육내용 • 개인정보보호 준수, 이행사항 • 개인정보보호지침 및 보호계획 이해 • 개인정보보호업무 절차, 책임, 방법 등 • 개인정보보호시스템 내용, 사용방법 숙지
개인정보 보호법 교육 결과보고 (시행문)	△ △ △ 기관 OO 기관 수신자 (경유) 제목 개인정보보호법 주요내용 및 이행사항 교육결과 보고 1. 관련 - 행정안전부 개인정보보호과-964(2012.2.9) 「개인정보보호법 주요내용 및 이행사항 교육자료 송부」 - 고용노동부 정보화기획팀-628(2012.2.9) 「개인정보보호법 주요내용 및 이행사항 교육자료 송부」 2. 귀청 관련하여 개인정보보호법 주요내용과 이행사항에 대한 교육을 실시하고 결과를 다음과 같이 보고합니다. 가. 교육기간 : 2012. 2.14(월) ~ 3.2(금) 나. 교육인원 : 1,164명 다. 교육방법 : 정보화담당자 회의참여시 담당자 교육후 전파교육 실시 붙임 : 개인정보 이행사항 교육결과 1부. 끝. 공공기관

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제26조(업무위탁에 따른 개인정보의 처리제한)

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.

제28조(개인정보취급자에 대한 감독)

② 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

제31조(개인정보 보호책임자의 지정)

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적 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. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

【개인정보의 안전성 확보조치 기준 고시】

제4조(내부 관리계획의 수립·시행)

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

3. 개인정보취급자에 대한 교육에 관한 사항

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제28조
- 개인정보의 안전성 확보조치 기준 해설서 – 제2장 제4조

3 개인정보 침해대응

세부분야	침해사고 신고방법 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.3.1	● **개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?**	○			
평가 예시	● 이행 : 개인정보 침해신고 절차를 수립하고, 침해신고 방법을 홈페이지(개인정보처리방침 등)에 안내하고 있는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 홈페이지의 개인정보 처리방침 '10조 개인정보보호책임자' 항목에서 침해사실을 신고할 수 있는 내부 부서를 안내하고 있고, '11조 개인정보 열람청구' 항목에 외부 기관에 침해사고 신고방법을 안내하고 있음				

주요 점검 사항

1. 개인정보 침해(권리 침해, 개인정보 유출 등)에 대해 신고할 수 있는 방법을 정보주체가 쉽게 확인할 수 있도록 안내하여야 한다.

지표 해설

- 정보주체의 권리 침해, 개인정보 유출 등 개인정보 침해 사실을 신고할 수 있는 방법을 개인정보처리방침 또는 인터넷 홈페이지의 별도 메뉴 등을 통하여 정보주체가 쉽게 확인할 수 있도록 안내하여야 한다.
- 개인정보처리자의 개인정보 처리로 인해 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보보호위원회에 그 침해 사실을 신고할 수 있다. 권리·이익을 침해받은 정보주체 자신뿐만 아니라 그의 법정대리인이나 임의대리인도 정보주체를 대신하여 신고할 수 있다.
- 개인정보보호위원회는 개인정보 침해신고 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 한국인터넷진흥원(KISA)을 전문기관으로 지정하고 있으며(영 제59조), 이에 따라 한국인터넷진흥원은 개인정보 침해 신고센터(http://privacy.kisa.or.kr)를 설치·운영하고 있다. 개인정보침해 신고센터는 개인정보 처리와 관련한 신고의 접수·상담, 접수된 사건에 대한 사실의 조사·확인 및 관계자 의견청취, 그 밖에 이들 업무와 관련된 부수적 업무를 수행한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.3.1	개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?	○			
평가근거 및 의견	● △△△ 기관은 홈페이지의 개인정보 처리방침 '10조 개인정보보호책임자' 항목에서 침해사실을 신고할 수 있는 내부 연락처를 안내하고 있고, '11조 개인정보 열람청구'항목에 외부 기관에 침해사고 신고 방법을 안내하고 있음				

개인정보 처리방침	
	③ 아래의 기관은 는 별개의 기관으로서, 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 사이버범죄수사단 : 1566-0112 (www.netan.go.kr)

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제30(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.

5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정하는 사항

제34(개인정보의 유출통지 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 개인정보보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 개인정보보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제62조(침해사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보보호위원회에 그 침해 사실을 신고할 수 있다.

② 개인정보보호위원회는 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.

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 개인정보보호위원회는 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.

【개인정보 보호법 시행령】

제31조(개인정보 처리방침의 내용 및 공개방법) ① 법 제30조제1항제8호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 처리하는 개인정보의 항목
2. 삭제
3. 제30조 또는 제48조의2에 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

제59조(침해사실의 신고 등) 개인정보보호위원회는 법 제62조제2항에 따라 개인정보에 관한 권리 또는 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위한 전문기관으로 한국인터넷진흥원을 지정한다.

【표준 개인정보 보호지침】

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

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

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제30조, 제34조, 제8장 제62조

세부분야	유출사고 대응				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.3.2	● **개인정보 유출 신고·통지 절차, 긴급 연락체계, 사고 대응 조직 구성 등을 포함한 개인정보 침해사고 대응절차를 수립하여 실시하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보 침해사고에 대비한 대응절차를 수립하고 있으나, 게시판 게시, 교육을 통한 내용 전파 등 전 직원에게 침해사고 대응절차를 전파하지 않는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '침해사고 대응 지침'을 통해 침해사고시 조치방법, 업무분장 및 연락처 등 침해사고에 대한 대응절차가 마련되어 있으나, 게시판 등에 게시하지 않고 교육을 통해 안내하지도 않는 등 직원에게 전파하지 않음				

주요 점검 사항

1. 개인정보 침해사고(권리침해, 개인정보 유출 등)에 대한 대응절차가 마련되어 내부 승인절차를 통해 공식적으로 시행되어야 한다.
2. 개인정보 침해사고 대응절차에는 아래와 같은 사항이 모두 포함되어야 한다.
   ① 개인정보 유출 시 신고 및 통지 절차
   ② 비상연락망 등 긴급 연락체계
   ③ 사고 대응조직 구성 및 업무분장(R&R)
   ④ 침해사고 유형별 조치 방법 및 절차
   ⑤ 정보주체 피해구제 방법
3. 개인정보 침해사고 대응절차를 이해관계자들이 인지할 수 있도록 공유하여야 한다.
4. 개인정보 침해사고에 대비한 모의훈련을 연 1회 이상 정기적으로 실시해야 한다.(권고사항)

지표 해설

- 개인정보 유·노출 및 침해사고를 통하여 발생할 수 있는 사회적, 경제적 피해 등 2차 피해를 예방하기 위하여 개인정보 침해사고 대응 범위, 절차, 담당자·부서별 업무, 피해구제 방법, 비상연락망·연락체계 등 침해사고 대응절차 마련을 권장한다.
  1. 침해사고 시 조치방법
  2. 업무분장 및 연락체계
  3. 유출통지 등 침해구제 방법
  4. 침해신고 방법
- 개인정보 유출사고 발생 시 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 포함하여 유출사실을 통보하고, 유출 확산방지를 위한 기술적 · 관리적 조치 등의 유출사고에 대응 할 수 있는 절차를 수립하고 실시하여야 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

- 1천명 이상의 개인정보 유출 사고 발생 시 기관은 정보주체에 대한 통지 및 조치결과를 5일 이내에 개인정보보호위원회 또는 전문기관(한국인터넷진흥원)에 유출사고 사실을 신고하고, 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 위 사항을 포함한 유출사실을 7일 이상 게재하여야 한다.
- 유출사고 발생 시 기관이 대응하기 위해 필요한 모든 내용을 포함하고 있는 절차를 수립하여야 한다. 접속경로 차단, 시스템 일시정지, 암호 등의 변경, 유출 원인 분석, 유출된 개인정보의 삭제, 기술적 보안조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 임시 대응조치에서부터 유사사고 발생 방지대책 수립 및 시행 등과 같은 장래의 피해 예방조치 등을 포함하여야 한다.
- 침해사고에 대비하여 개인정보취급자 대상 교육 및 모의훈련 실시, 사내 정보시스템 (인트라넷) 게시 등으로 신속하고 효율적으로 대응할 수 있는 체계를 구축할 것을 권장한다.

용어설명

※ 개인정보 유출 : 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것

- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
- 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
- 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
- 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

※ 개인정보 노출 : 일반 인터넷 이용자가 해킹 등 특별한 방법을 이용하지 않고, 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷 등에 방치되는 경우

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.3.2	개인정보 유출 신고·통지 절차, 긴급 연락체계, 사고 대응 조직 구성 등을 포함한 개인정보 침해사고 대응절차를 수립하여 실시하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 '침해사고 대응 지침'을 통해 침해사고시 조치방법, 업무분장 및 연락처 등 침해사고에 대한 대응절차가 마련되어 있으나, 게시판 등에 게시하지 않고, 교육을 통해 안내하지 않는 등 직원에게 전파하지 않음.				

침해사고 대응 지침	목 차
	제1조 (목적) ····· 1 제2조 (적용범위) ····· 1 제3조 (용어의 정의) ····· 1 제4조 (책임사항) ····· 3 제5조 (유관기관 연계절차 및 외부 인터넷보안센타와의 연계방안) ····· 3 제6조 (보안사고 예방활동) ····· 4 제7조 (사이버침해사고 대응절차) ····· 6 제8조 (사이버위기경보 대응절차) ····· 8 제9조 (개인정보 유출사고 대응절차) ····· 9 제10조 (이메일 침해사고 대응절차) ····· 10 제11조 (보안취약성 대응절차) ····· 11 제12조 (긴급대응반의 편성·운영) ····· 11

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제34조(개인정보의 유출통지 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 개인정보보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 개인정보보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제62조(침해사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다.

② 보호위원회는 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.

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 개인정보보호위원회는 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.

【개인정보 보호법 시행령】

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

② 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 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 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1천명 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.

【표준 개인정보 보호지침】

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 저장매체가 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 개인정보처리자는제1항 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. 제27조제1항의 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 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 개인정보보호위원회 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지제1호서식에 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제34조, 제8장 제62조

4 정보주체 권리보장

세부분야	정보주체 권리보장 절차 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.4.1	● **개인정보 열람, 정정·삭제 및 처리정지, 수집출처 고지 등 정보주체의 요구에 대한 처리절차를 수립하여 실시하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보 열람, 정정·삭제 및 처리정지에 대한 일부 절차만 수립하고 있거나, 일부 절차만 실시하고 있는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '개인정보보호지침'의 '5장 정보주체의 권리보장'에 개인정보의 열람, 정정, 삭제 요청에 대한 처리 절차를 수립하고 있으나, 처리정지 및 수집 출처 고지 관련 요구에 대한 처리 절차는 누락되어 있음				

주요 점검 사항

1. 정보주체의 개인정보 열람, 정정·삭제, 처리정지, 수집출처 요구에 대하여 대응할 수 있는 처리절차를 수립하여 공식적으로 시행하여야 한다.
2. 정보주체 요구 처리절차에는 아래와 같은 사항이 모두 포함되어야 한다.
   ① 정보주체 요구 유형(열람, 정정·삭제, 처리정지, 수집출처 요구)에 따른 대응 절차
   ② 정보주체 요구 접수 부서 및 담당자
   ③ 정보주체 요구 관리대장 양식
   ④ 정보주체 또는 법정대리인 본인 여부를 확인할 수 있는 절차
   ⑤ 정보주체 요구 거절 기준 및 이에 따른 절차 등
3. 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 한다.
4. 정보주체 권리보장 절차를 이해관계자들이 준수할 수 있도록 공유하여야 한다.
5. 개인정보처리자가 개인정보보호법 제17조제1항제1호(제3자 제공 동의)에 따라 정보주체 이외로부터 수집한 경우 개인정보보호법 시행령 제15조의2 제1항에 해당하는 개인정보처리자는 정보주체에게 수집 출처 고지 등 의무를 준수하여야 한다. (이 경우는 해당하는 개인정보처리자에 한함)

지표 해설

- 정보주체의 개인정보 열람, 정정·삭제 및 처리정지에 대한 처리 절차를 수립하여야 하며 관련된 신청 양식을 만들고 신청을 처리한 내역을 기록하고 관리하여야 한다.
- 열람에는 사본의 교부를 포함하며, 정보주체가 직접 제공한 개인정보 이외에 제3자 또는 공개된 소스로부터 수집한 개인정보, 개인정보처리자가 생산한 개인정보(신용평가, 인사평가, 거래내역, 진료기록 등), 서비스제공 등의 과정에서 자동적으로 생성된 개인정보(수발신 내역, 입출기록, 쿠키, 로그기록 등) 등도 열람요구의 대상이 된다.

- 개인정보 열람, 정정·삭제 및 처리정지 요청에 대한 처리절차는, 법률에서 정한 열람, 정정, 삭제 및 처리정지 등의 요구가 제외되는 대상을 정의하고, 정보주체의 요구가 정당하게 거부되었음을 고지하는 절차를 포함하여 수립하여야 한다.

- 개인정보 열람, 정정 및 삭제 처리에 대한 정보주체의 요구에 대하여, 정당한 사유가 없는 한 10일 이내에 열람, 정정 및 삭제에 대한 처리결과를 정보주체에게 알려야 한다.

열람요구 항목(영 제41조 제1항)
1. 개인정보의 항목 및 내용 2. 개인정보의 수집·이용의 목적 3. 개인정보 보유 및 이용 기간 4. 개인정보의 제3자 제공 현황 5. 개인정보 처리에 대하여 동의한 사실 및 내용

열람 제한 · 거절 사유(법 제35조 제4항)
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

- 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실 등을 알려야 한다. "표준 개인정보 보호지침"에서는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 관련 사항을 정보주체에게 알리도록 명시하고 있다.

- 「개인정보 보호법」 제20조제2항에 따라 정보주체의 제3자 제공 동의에 근거하여 개인정보를 제공받아 처리하는 때에는 정보주체의 요구가 없더라도 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실 등을 정보주체에게 알려야 한다.

정보주체 이외로부터 수집한 개인정보 출처 고지 의무(시행령 제15조의2)
1. 대상 - 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보 또는 법 제24조제1항에 따른 고유식별정보를 처리하는 자 - 100만 명 이상의 정보주체에 관하여 개인정보를 처리하는 자 2. 고지 방법 - ① 수집 출처, ② 처리 목적, ③ 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 개인정보를 제공받은 후 3개월 이내에 정보주체에게 알려야 한다. - 서면·전화·문자전송· 전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 알려야 하고, 정보주체에게 알린 사실을 (시기 및 방법을 포함한다) 해당 정보를 파기할 때까지 관리하여야 한다.

- 정보주체가 열람 등을 요구할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

- 정보주체의 권리행사 방법 및 절차는 최소한 개인정보 수집절차 또는 회원가입 절차에 준해서 알기 쉽고 편리하여야 하며, 개인정보 수집 시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구해서는 안 된다. 또한, 정보주체가 편리하게 선택할 수 있도록 가급적 다양한 권리행사 방법을 마련하여 제공하여야 한다. 예컨대 방문, 서면, 전화, 전자우편, 인터넷 웹사이트 등 다양한 방법으로 정보주체가 열람·정정·삭제·처리정지 등을 요구할 수 있도록 하여야 한다.

- 개인정보처리자는 개인정보 열람요구, 정정·삭제요구, 처리정지요구, 수집출처 요구 등을 받은 때에는 열람 등의 요구를 한 자가 본인이거나 정당한 대리인인지를 확인하여야 한다. 대리인의 경우에는 대리인 자신에 관한 신원확인뿐만 아니라 정보주체와 대리인 사이의 대리관계를 증명할 수 있는 위임장 및 인감 또는 법정대리인의 경우에는 법정대리인임을 확인할 수 있는 서면(주민등록등본, 가족관계증명서 등)을 추가로 확인하여야 한다.

- 신원확인의 방법은 별도로 특정되어 있지 않다. 따라서 인터넷의 경우에는 아이디/비밀번호, 전자서명, 휴대폰 본인확인, 아이핀 등의 방법에 의해서 확인하면 되고, 오프라인의 경우에는 주민등록증, 운전면허증, 여권, 공무원증 등에 의하면 된다. 즉 합리적인 수단이라고 객관적으로 인정되는 방식에 의해서 하면 된다.

- 개인정보처리자가 공공기관인 경우에는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 신분확인이 가능하면 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

- 정보주체가 사용하는 홈페이지 등의 경우에 로그인을 통해 1차 본인확인 과정을 거치지만 로그인 후 사용자 실수, 불법적인 계정 탈취 및 노출 등으로 정보주체가 원치 않는 정보 수정, 비밀번호 변경, 회원탈퇴 등이 발생할 수 있으므로, 본인정보 수정, 비밀번호 변경, 회원탈퇴 등을 처리하는 사항에서는 비밀번호 재확인 등 추가 인증을 구현하여 비인가자 접근 또는 정보주체의 실수로 발생할 수 있는 일들을 사전에 방지할 수 있다.

- 정보주체가 사용하는 홈페이지 등을 통해 민감한 정보가 포함된 이용 내역 열람이나, 포인트 사용 등 비인가자 접근 또는 정보주체의 실수 발생 시 정보주체의 피해가 발생할 수 있는 사항에 대해서도 추가적인 인증을 구현할 수 있다.

- 개인정보처리자는 정보주체의 권리행사 방법과 절차를 어렵게 하거나 정보주체에게 과도한 비용을 청구하여서는 안 된다. 그러나 정보주체 이외의 자가 권한없이 또는 권한을 넘어 정보주체의 권리를 대신하여 행사하지 못하도록 적절한 수준의 본인확인 절차를 강구하여야 한다.

- 개인정보처리자는 정보주체가 열람 등을 요구할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다. 다수의 정보주체들이 자신의 권리를 알지 못하고, 알고 있는 경우에도 절차가 까다롭고 복잡해 포기하는 경우가 많다. 따라서 정보주체의 권리행사 방법 및 절차는 최소한 개인정보 수집 절차 또는 회원가입 절차에 준해서 알기 쉽고 편리해야 하며, 개인정보 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구해서는 안 된다(표준지침 제34조). 또한, 정보주체가 편리하게 선택할 수 있도록 가급적 다양한 권리행사 방법을 마련하여 제공해야 한다. 예컨대 방문, 서면, 전화, 전자우편, 인터넷 웹사이트 등 다양한 방법으로 정보주체가 열람, 정정·삭제, 처리정지 등을 요구할 수 있도록 해야 한다.

- 정보주체는 개인정보처리자가 자신에 관하여 어떤 정보를 보유하고 있고, 어떻게 활용하고 있으며, 개인정보처리자가 보유하는 개인정보는 정확한지 여부를 확인할 수 있어야 한다. 이와 같은 정보주체의 권리는 개인정보자기통제권의 핵심을 이룬다.

- 허위 또는 부정확한 정보로부터 정보주체의 권리를 보호하기 위하여 잘못된 개인정보에 대한 정정 또는 삭제를 요구할 수 있는 권리를 정보주체에게 부여하고자 한 것이다. 그러나 정보의 일방적인 정정·삭제는 또 다른 문제를 낳을 수 있으므로 그 행사에는 일정한 제약이 따른다.

- 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 처리정지 요구권은 개인정보처리 활동에 대한 정지를 요구하는 것으로 동의 철회권보다는 그 개념이 넓다. 동의 철회권은 정보주체 자신이 동의한 것에 대해서만 동의를 철회할 수 있으나, 처리정지 요구권은 정보주체 자신이 처리에 동의하지 아니한 것에 대해서는 처리정지를 요구할 수 있는 일종의 법정 해지권과 같은 성격의 것이라고 할 수 있다. 정보주체는 처리정지 요구의 이유를 댈 필요가 없으며 언제든지 요구가 가능하다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.4.1	개인정보 열람, 정정·삭제 및 처리정지, 수집출처 고지 등 정보주체의 요구에 대한 처리절차를 수립하여 실시하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 '개인정보보호지침'의 '5장 정보주체의 권리보장'에 개인정보의 열람, 정정, 삭제 요청에 대한 처리 절차를 수립하고 있으나, 처리정지 및 수집 출처 고지 관련 요구에 대한 처리 절차는 누락되어 있음				

개인정보 보호지침	제5절 정보주체의 권리 보장 **제30조(개인정보 열람 연기 사유의 소멸)** 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다. ② 정보주체로부터 시행령 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공현황의 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. **제31조(개인정보의 정정·삭제)** ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때에는 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.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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

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.

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

④ 제1항과 제2항 본문은 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

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 개인정보보호위원회를 통하여 열람을 요구할 수 있다.

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, 제39조의7에 따른 동의 철회 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 열람등 요구를 할 수 있다.

③ 개인정보처리자는 열람등 요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.

④ 개인정보처리자는 정보주체가 열람등 요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ 개인정보처리자는 정보주체가 열람등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

【개인정보 보호법 시행령】

제15조의2(개인정보 수집 출처 등 고지대상·방법·절차) ① 법 제20조제2항 본문에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 "고유식별정보"라 한다)를 처리하는 자
2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

② 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 법 제20조제1항 각 호의 사항을 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다. 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 한다.

제41조(개인정보의 열람절차 등) ① 법 제35조제1항에 따라 자신의 개인정보에 대한 열람을 요구하려면 다음 각 호의 사항 중 열람하려는 사항을 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다.

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 개인정보처리자는 제1항에 따른 열람 요구 방법과 절차를 마련하는 경우 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 다음 각 호의 사항을 준수하여야 한다.

1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

③ 정보주체가 법 제35조제2항에 따라 개인정보보호위원회를 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 개인정보보호위원회가 정하여 고시하는 바에 따라 제1항 각 호의 사항 중 열람하려는 사항을 표시한 개인정보 열람요구서를 개인정보보호위원회에 제출하여야 한다. 이 경우 개인정보보호위원회는 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송하여야 한다.

④ 법 제35조제3항 전단에서 "대통령령으로 정하는 기간"이란 10일을 말한다.

⑤ 개인정보처리자는 제1항 및 제3항에 따른 개인정보 열람 요구를 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 개인정보보호위원회가 정하여 고시하는 열람통지서로 해당 정보주체에게 알려야 한다. 다만, 즉시 열람하게 하는 경우에는 열람통지서 발급을 생략할 수 있다.

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 개인정보보호위원회가 정하여 고시하는 열람의 연기·거절 통지서로 해당 정보주체에게 알려야 한다.

제43조(개인정보의 정정·삭제 등) ① 정보주체는 법 제36조제1항에 따라 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 정정 또는 삭제 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, "열람"은 "정정 또는 삭제"로 본다.

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·삭제에 관한 요구 사항을 해당 개인정보를 제공한 기관의 장에게 지체 없이 알리고 그 처리 결과에 따라 필요한 조치를 하여야 한다.

③ 개인정보처리자는 제1항과 제2항에 따른 개인정보 정정·삭제 요구를 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 개인정보보호위원회가 정하여 고시하는 개인정보 정정·삭제 결과 통지서로 해당 정보주체에게 알려야 한다.

제44조(개인정보의 처리정지 등) ① 정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 처리 정지 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, "열람"은 "처리 정지"로 본다.

② 개인정보처리자는 제1항에 따른 개인정보 처리정지 요구를 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 개인정보보호위원회가 정하여 고시하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.

【개인정보 처리방법에 관한 고시】

제3조(개인정보 보호업무 관련 장부 및 문서 서식) ⑥ 법 제35조제2항과 영 제41조제3항에 따른 개인정보 열람의 요구는 별지 제8호서식의 개인정보 열람 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.

【표준 개인정보 보호지침】

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.

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제20조, 제5장(정보주체의 권리보장)

세부분야	정보주체 권리보장 방법 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
1.4.2	● **정보주체의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보 열람, 정정·삭제, 처리정지 처리결과에 대한 불복 청구 절차와 방법을 인터넷 홈페이지·관보 등을 통해 정보주체에게 안내하고 있지 않은 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 개인정보처리방침 '제4조 정보주체의 권리·의무 및 그 행사 방법' 5항에서 개인정보의 열람, 정정 · 삭제, 처리정지 요청방법은 안내하고 있으나 불복 청구 절차 및 방법은 안내하고 있지 않음				

주요 점검 사항

1. 정보주체의 개인정보 열람, 정정·삭제, 처리정지, 수집출처 요구에 대한 개인정보처리자의 조치에 불복이 있는 경우 이의를 제기할 수 있는 절차를 마련해야 한다.
2. 정보주체의 요구에 대한 처리결과 통지 시에, 처리 결과에 대한 불복이 있는 경우 이의를 제기할 수 있는 방법을 함께 안내하여야 한다.

지표 해설

- 열람 등의 요구에 대한 거절 조치에 대하여 불복이 있는 경우 정보주체가 이의를 제기할 수 있도록 개인정보처리자는 필요한 절차를 마련하고 안내하여야 한다. 이 경우 이의제기 절차는 공정하게 운영될 수 있도록 외부 전문가를 참여시키거나 내부의 견제장치가 마련되어 있어야 한다.
- 정보주체의 개인정보 열람, 정정·삭제, 처리정지, 수집출처 요구 등에 대한 처리 결과를 통지할 때에는 처리 결과에 불복이 있는 경우 이에 대한 이의를 제기할 수 있는 방법을 함께 안내하는 것이 권고된다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
1.4.2	정보주체의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하고 있습니까?			○	
평가근거 및 의견	● △△△ 기관은 개인정보처리방침 '제4조 정보주체의 권리·의무 및 그 행사 방법' 5항에서 개인정보의 열람, 정정 · 삭제, 처리정지 요청방법은 안내하고 있으나 불복 청구 절차 및 방법은 안내하고 있지 않음.				

개인정보 처리방침	제6조 : 정보주체의 권리, 의무 및 그 행사방법 정보주체는 개인정보주체로서 다음과 같은 권리를 행사할 수 있습니다. ①정보주체는 <한국산업안전보건공단>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 ②제1항에 따른 권리 행사는 <한국산업안전보건공단>에 대해 개인정보 보호법 시행규칙 별지 제8호 서식에 따라 서면, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며 <한국산업안전보건공단>은 이에 대해 지체 없이 조치하겠습니다. ③정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 <한국산업안전보건공단>은 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않습니다. ④제1항에 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.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제38조(권리행사의 방법 및 절차)

⑤ 개인정보처리자는 정보주체가 열람등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제5장 정보주체의 권리보장

2. 대상시스템의 개인정보보호 관리체계

1 개인정보취급자 관리

세부분야	개인정보취급자 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.1.1	● **업무상 필요한 최소한의 범위로 최소한의 인원이 개인정보를 처리하도록 개인정보 취급자를 지정하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 일부 개인정보 취급인원만 개인정보취급자로 지정하도록 계획하는 경우, 또는 개인정보취급자 명단을 관리하고 있지 않거나, 개인정보취급자가 지정사실을 모르는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관의 ○○○시스템의 개인정보취급자를 '○○○시스템 개인정보취급자 명단'으로 관리하고 있으나 인사공문에서 확인한 20XX년 XX월 퇴사한 김○○이 개인정보취급자 명단에 기재되어 있음				

주요 점검 사항

1. 개인정보취급자는 업무상 필요한 최소한의 범위로 지정할 수 있도록 지정기준을 마련하여 시행하여야 한다.
2. 개인정보취급자를 목록으로 관리하여야 하며, 개인정보취급자 목록에는 개인정보를 처리하는 모든 인원(임직원, 파견 근로자, 시간제 근로자 등)이 포함되어야 한다.

지표 해설

- 개인정보취급자란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제 근로자 등을 말한다. 표준지침에서는 이를 구체화하여, 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 의미한다고 규정하고 있다.
- 즉, 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면 정규직, 비정규직, 하도급, 시간제 등 모든 근로형태를 불문한다. 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다.
- 개인정보 처리업무 등을 위탁받아 처리하고 있는 수탁자도 개인정보취급자라고 할 수 있으나, 수탁자에 대한 교육 및 관리·감독규정은 「개인정보 보호법」 제26조에서 별도로 규정하고 있으므로 그에 따른다.
- 개인정보취급자의 범위를 최소한으로 제한하고, 그들에 의한 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한할 수 있도록 취급자의 지정 기준을 정한다. 이때 개인정보취급자는 기관별 여건을 고려하여 규정, 지침 등에 지정 기준을 정할 것을 권장한다.

- 이를 위해 개인정보처리자는 개인정보취급자의 범위를 최소한으로 제한하고, 그들에 의한 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한하여야 하고(표준지침 제15조제1항), 또한 개인정보 처리시스템에 접근할 수 있는 권한을 업무수행에 필요한 최소한의 범위에서 관련 업무담당자에게 차등적으로 부여하는 등 개인정보 처리시스템 접근권한을 관리하여야 한다.(표준지침 제15조제2항)

- 기관의 정확한 개인정보취급자 현황을 파악하기 위해서는 개인정보취급자 명단을 작성하여 관리할 것을 권장한다.
  - 업무상 개인정보를 취급하여야 하는 개인정보취급자는 최소한으로 제한하고, 개인정보취급자 명단 관리 방안 및 통제방안을 마련할 것을 권장한다.
  - 작성된 개인정보취급자 명단을 통해 보안서약서가 누락되었거나 잘못된 계정 권한 발급 등을 점검하여 개인정보취급자를 최소한으로 제한할 수 있도록 감독할 것을 권장한다.

용어설명

※ 개인정보취급자 : 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.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
2.1.1	업무상 필요한 최소한의 범위로 최소한의 인원이 개인정보를 처리하도록 개인정보 취급자를 지정하도록 계획하고 있습니까?		○		

평가근거 및 의견

● △△△ 기관의 ○○○시스템의 개인정보취급자를 '○○○시스템 개인정보취급자 명단'으로 관리하고 있으나 인사공문에서 확인한 20XX년 XX월 퇴사한 김○○이 개인정보취급자 명단에 기재되어 있음.

○○○시스템 개인정보 취급자 명단

개인정보취급자 명단

시스템 명 : 000000 시스템 2013.03.01

연번	성명	소속	직급	계정 ID	접근권한				비고
					등급(전)	등급(후)	등록일자	말소일자	
1	김	1과	과장	u	[illegible]	000	[illegible]		
2	김	1과	선임	u	[illegible]			2013.02.01	
3	백	1과	선임	1c	[illegible]				
4	김	1과	주임	o	[illegible]				
5	정	1과	주임	ox	[illegible]				
6	김	1과	주임	d	[illegible]				
7	수	1과	주임	o	[illegible]				
8	김	1과	선임	ok	[illegible]				
9	김	1과	주임	o	[illegible]	000			

인사 공문

수신 내부결재
(경유)
제목 상반기 정기 인사명령

2011년 상반기 정기 인사명령을 아래 다음과 같이 발 함.

- 다 음 -

~ 을				발령사항	~ 으로	
성 명	부 서	직 급	사 번	발령구분	부 서	직 급
홍						대리
김				퇴사		

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제28조

세부분야	개인정보취급자 관리·감독				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.1.2	● **개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호 서약서 작성 등 관리·감독을 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보취급자의 업무가 문서로 정의되어 있으나, 법률요건 중 일부만 반영하였거나, 개인정보보호 교육 및 서약서 작성 시 누락 인원이 존재하는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '개인정보보호지침'에서 개인정보취급자에 대한 업무를 부여하고 있으나 법에서 요구하는 '개인정보 보호책임자에게 개인정보 파일 등록 신청'에 관한 사항은 누락되어 있음				

주요 점검 사항

1. 개인정보취급자에게 법률에서 규정된 업무(역할 및 책임)를 공식적으로 부여해야 한다.
2. 대상시스템에서 업무를 처리하는 개인정보취급자를 대상으로 개인정보보호 교육을 연1회 이상 정기적으로 수행하여야 한다.
3. 개인정보보호 교육을 이수한 개인정보취급자 목록을 관리해야 하며, 교육 미이수자에 대한 조치방안(재교육, 전달교육 등)이 존재해야 한다.
4. 개인정보취급자를 대상으로 개인정보보호 서약서를 작성하도록 하며, 사고 발생 등을 대비하여 이를 보관하여야 한다.
5. 개인정보취급자 목록 검토, 개인정보보호 서약서 작성 여부 점검, 개인정보보호 교육 이수 현황 점검 등 개인정보취급자에 대한 정기적인 관리·감독 계획을 수립하고 시행해야 한다.

지표 해설

● 개인정보취급자에게 법률 등에서 규정된 업무를 공식적으로 부여하여야 한다.

개인정보취급자의 역할 및 책임
1. 개인정보 처리 2. 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무 3. 개인정보 보호책임자에게 개인정보 파일 등록 신청 4. 개인정보파일 파기 5. 개인정보 파기 시 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청 6. 개인정보보호 활동 참여 7. 내부 관리계획의 준수 및 이행 8. 개인정보의 기술적·관리적 보호조치 기준 이행 9. 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

- 기관의 정확한 개인정보취급자 현황을 파악하기 위해서는 개인정보취급자 명단을 작성하여 관리하고, 개인정보취급자 명단 관리방안 및 통제방안을 마련할 것을 권장한다.

- 작성된 개인정보취급자 명단을 통해 보안서약서가 누락되었거나 잘못된 계정 권한 발급 등을 점검하여 개인정보취급자를 최소한으로 제한할 수 있도록 감독할 것을 권장한다.

- 개인정보처리자는 개인정보를 처리함에 있어서 개인정보에 대한 무분별한 접근권한 부여로 인하여 개인정보의 접근 및 유출, 오·남용이 발생하는 것을 방지하기 위하여 개인정보가 안전하게 관리될 수 있도록 개인정보취급자에 대하여 적절한 관리·감독을 행하여야 한다.

- 적절한 관리·감독은 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 각기 달라져야 한다. 또한 관리·감독은 1회성으로 그쳐서는 안 되고 조직적·체계적으로 이루어져야 하며 반드시 평가·피드백 시스템이 강구되어야 한다.

- 이를 위해 개인정보처리자는 개인정보취급자의 범위를 최소한으로 제한하고, 그들에 의한 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한하여야 하고(표준지침 제15조제1항), 또한 개인정보처리시스템에 접근할 수 있는 권한을 업무수행에 필요한 최소한의 범위에서 관련 업무담당자에게 차등적으로 부여하는 등 개인정보 처리시스템 접근권한을 관리하여야 한다(표준지침 제15조제2항). 그 외에 개인정보취급자에 대한 관리·감독의 방안으로 보안서약서 제출 등을 의무화하고, 개인정보취급자가 변경된 경우 접근권한의 변경 등 관리방안을 구체적으로 마련하여야 한다(표준지침 제15조제3항).

개인정보취급자에 대한 관리 감독
1. 개인정보처리자는 개인정보를 처리함에 있어서 개인정보에 대한 무분별한 접근권한 부여로 인하여 개인정보의 접근 및 유출, 오·남용이 발생하는 것을 방지하기 위하여 개인정보가 안전하게 관리될 수 있도록 개인정보취급자에 대하여 적절한 관리·감독을 행하여야 한다. 2. 적절한 관리·감독은 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 각기 달라져야 한다. 또한 관리·감독은 1회성으로 그쳐서는 안 되고 조직적·체계적으로 이루어져야 하며 반드시 평가·피드백 시스템이 강구되어야 한다. 이를 위해 개인정보처리자는 개인정보취급자의 범위를 최소한으로 제한하고, 그들에 의한 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한하여야 하고(표준지침 제15조제1항). 또한 개인정보 처리시스템에 접근할 수 있는 권한을 업무수행에 필요한 최소한의 범위에서 관련 업무담당자에게 차등적으로 부여하는 등 개인정보 처리시스템 접근권한을 관리하여야 한다(표준지침 제15조제2항). 그 외에 개인정보취급자에 대한 관리·감독의 방안으로 보안서약서 제출 등을 의무화하고, 개인정보취급자가 변경된 경우 접근권한의 변경 등 관리방안을 구체적으로 마련하여야 한다(표준지침 제15조제3항).

- 개인정보처리자의 점검항목에는 다음 사항을 포함하여야 하며, 외부 인력에 대한 점검을 포함하여야 한다.
  1. 개인정보취급자의 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한하고 있는지 여부
  2. 개인정보 처리시스템에 접근할 수 있는 권한을 업무수행에 필요한 최소한의 범위에서 관련 업무담당자에게 차등적으로 부여하는지 여부
  3. 개인정보취급자의 보안서약서 제출 여부
  4. 개인정보취급자가 변경된 경우 접근권한의 변경 여부

- 개인정보처리자의 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다. 이러한 개인정보보호 교육계획은 내부 관리계획 및 개인정보보호 연간계획에 포함하여 실행력을 확보할 필요가 있으며, 모든 개인정보취급자가 관련 교육을 이수할 수 있도록 교육 참석 현황을 관리하고 미 이수자에 대한 교육방안(재교육, 전달교육 등)도 마련하여야 한다.

개인정보취급자에 대한 정기적인 교육
개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다. 교육은 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으나 연간 교육계획을 수립하여 모든 개인정보취급자가 일정 시간 이상 교육에 참여하도록 해야 한다. 또한 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 교육 내용도 각기 달라져야 한다.

평가 예시

<table>
<tr><th>구 분</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>2.1.2</td><td>개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호 서약서 작성 등 관리·감독을 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가근거 및 의견</td><td colspan="5">● △△△ 기관은 '개인정보보호지침'의 '5.나 개인정보취급자의 업무' 항목에서 개인정보취급자에 대한 업무를 부여하고 있으나 법에서 요구하는 '개인정보 보호책임자에게 개인정보 파일 등록 신청'에 관한 사항은 누락되어 있음.
<table>
<tr><td>개인정보 보호지침</td><td>나. 개인정보취급자의 업무
- 개인정보처리
- 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무
- 개인정보보호 활동 참여
- 개인정보파일 파기
- OO부 개인정보 보호지침의 준수 및 이행</td></tr>
</table></td></tr>
</table>

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보의 안전성 확보조치 기준】

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항

【표준 개인정 보보호지침】

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.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

제55조(개인정보파일의 파기) 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.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제32조

2 개인정보파일 관리

세부분야	개인정보파일 대장 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.2.1	● **대상시스템에서 개인정보 파일을 신규로 보유하거나 변경하는 경우, 개인정보파일 대장을 작성하거나 변경하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보파일대장을 작성하여 관리하고 있으나, 일부 개인정보파일이 누락되어 있거나, 개인정보의 항목 등 일부 내용이 틀린 경우				
평가근거 및 의견	● ○○○ 기관은 △△시스템에서 운용하는 15개의 개인정보파일 중 14개만 개인정보파일대장에 관리하고 있고 개인정보보호 포털(www.privacy.go.kr)에 14개만 등록되어 있음				

주요 점검 사항

1. 개인정보파일을 신규로 보유하거나 변경하는 경우, 지체 없이 개인정보파일 대장을 작성하거나 변경하여야 한다.
2. 개인정보파일 대장은 개인정보파일별로 아래 사항들이 현행화되어 관리되어야 한다.
   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 처리방법
   ⑦ 개인정보의 보유기간
   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 「개인정보 보호법」 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
   ⑫ 「개인정보 보호법」 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보 파일의 경우에는 그 영향평가의 결과
   ⑬ 기타 공공기관에서 개인정보파일 관리를 위해 필요한 정보(등록자, 등록·변경 일시 등)

지표 해설

- 공공기관의 장이 개인정보파일을 운용하는 경우에는 개인정보보호위원회에 그 사실을 등록하여야 한다. 등록된 사항에 변경이 있는 경우에도 역시 그 내용을 등록하여야 한다. 개인정보파일 등록은 공공기관만 부담하는 의무이며 민간 부문의 기업·단체 등은 개인정보파일 등록의무가 적용되지 않는다.

- 개인정보파일 등록 시에는 다음 항목을 포함하여야 한다.

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. 개인정보파일을 운용하는 공공기관의 명칭
8. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 영 제41조에 따른 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

- 국가안보, 외교상 비밀 등 국가의 중대한 이익이나 범죄수사 등 공익 달성을 위한 개인정보파일은 이를 공개하지 않는 것이 보다 공익에 부합할 수 있다. 따라서 이러한 개인정보파일은 등록·공개 의무를 면제할 수 있다.(「개인정보 보호법」 제32조 제2항의 적용 예외사항 참조)

등록면제 개인정보 파일
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 사용 되는 개인정보파일 5. 다른 법령에 따라 비밀로 분류된 개인정보파일

- 개인정보파일대장 작성은 법적 필수사항은 아니지만, 해당 기관이 보유하고 있는 개인정보파일의 체계적인 관리를 위해서는 개인정보파일 대장을 작성하여 관리하는 것이 권고된다. 이를 통해 개인정보파일의 현황을 정확하게 파악하고 이에 따른 보호조치를 적절히 적용할 수 있다.

- 개인정보파일대장의 내용은 개인정보보호위원회에 등록하는 항목을 포함하여야 하며, 내부 관리를 위한 정보(담당자, 변경일시 및 변경이력, 특이사항 등)를 추가하여 작성하는 것이 바람직하다.

- 또한, 개인정보파일 운용에 따라 개인정보파일의 내용이 변경될 수 있으므로 년1회 이상 주기적으로 개인정보파일의 변경여부를 확인하여 변경된 사항이 있는 경우 개인정보파일 대장에 반영하고, 필요 시 개인정보보호위원회에 등록할 필요가 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
2.2.1	대상시스템에서 개인정보 파일을 신규로 보유하거나 변경하는 경우, 개인정보파일 대장을 작성하거나 변경하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 홈페이지 OOO 개인정보파일 대장의 개인정보 항목에 현재 보유하고 있지 않은 "주민등록번호"가 포함되어 있음 (2014년 8월 주민등록번호 수집 법정주의 시행에 따라 주민등록번호 보유의 법적근거가 없어 삭제 처리됨)				

개인정보 파일대장

개인정보파일명		회원정보 파일		
1. 업무분야			2. 단위업무	
3. 보유목적				
4. 보유근거(관련법령)				
5. 수집방법				
6. 대상개인범위				
7. 대상인원수			8. 보유기간	영구
9. 기록항목		ID, 비밀번호, 이름, 이메일, 주민등록번호		
10. 사용부서				
11. 열람예정일		수시 열람		
12. 열람청구부서 및 주소		재해통계분석팀		
13. 열람제한	(1)열람제한항목	모든항목		
	(2)열람제한사유	법률의한 제한(통계법)		
14. 이용, 제공기관명		없음	15. 이용, 제공근거	없음
16. 이용, 제공항목		없음		

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다.

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

【개인정보 보호법 시행령】

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

【표준 개인정보 보호지침】

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제32조

세부분야	개인정보파일 등록				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.2.2	● **대상시스템에서 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우, 보호위원회에 등록하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 신규 개인정보파일을 보호위원회에 등록 했으나 개인정보파일대장에 기재하지 않은 경우 또는 이와 반대의 경우, 보호위원회에 등록한 개인정보파일 혹은 개인정보파일대장 내용이 미흡한 경우				
평가근거 및 의견	● ○○○ 기관은 △△시스템에서 운용하는 15개의 개인정보파일 모두 개인정보보호 포털(www.privacy.go.kr)에 등록은 되어 있으나, 등록된 3개의 파일에서의 운영근거, 수집하는 개인정보 항목이 잘못 등록되어 있음				

주요 점검 사항

1. 공공기관은 개인정보파일을 신규로 보유하거나 변경하는 경우, 60일 이내에 보호위원회에 등록 또는 변경할 수 있도록 개인정보파일 등록·변경 절차를 마련하고 시행해야 한다.
2. 개인정보파일 등록시 아래 사항들이 포함될 수 있도록 해야 한다.
   ① 개인정보파일을 운용하는 공공기관의 명칭
   ② 개인정00보파일의 명칭
   ③ 개인정보파일의 운영 근거 및 목적
   ④ 개인정보파일에 기록되는 개인정보의 항목
   ⑤ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
   ⑥ 개인정보의 처리방법
   ⑦ 개인정보의 보유기간
   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 「개인정보 보호법」 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
   ⑫ 「개인정보 보호법」 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보 파일의 경우에는 그 영향평가의 결과

지표 해설

● "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- 데이터베이스 기준이 아닌 개인별 업무분장 또는 정보시스템에 의해 처리하는 단위 업무 수준을 말함
- 전자파일 형태 외에 민원서류 등 수기문서 포함

개인정보파일 구분 예시

- 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우 그 운용을 시작한 날부터 60일 이내에 보호위원회에 등록하여야 한다.

- 공공기관의 장이 개인정보파일을 운용하는 경우에는 보호위원회에 그 사실을 등록하여야 한다. 등록된 사항에 변경이 있는 경우에도 역시 그 내용을 등록하여야 한다. 개인정보파일 등록은 공공기관만 부담하는 의무이며 민간 부문의 기업·단체 등은 개인정보파일 등록의무가 적용되지 않는다.

- 개인정보파일 등록 의무가 있는 공공기관은 구체적으로 다음과 같다(표준지침 제49조).
  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

- 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 그 소속 기관의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 따로 정하도록 하고 있다. 이에 따라 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 이들 기관의 소속기관에서 관리하는 개인정보파일에 대해서는 해당 기관에서 정한 표준지침에 따른 등록, 공개 의무 여부 등을 파악하여 수행하여야 한다.

- 개인정보파일 등록업무를 실제 수행하는 것은 해당 공공기관의 개인정보 보호책임자이다. 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다. 이 경우 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하고, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 등록하여야 한다. 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다(표준지침 제51조).

- 개인정보파일 등록 시에는 다음 항목을 포함하여야 한다.

개인정보파일 등록 시 포함해야 하는 항목
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. 개인정보파일을 운용하는 공공기관의 명칭 8. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수 9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서 10. 영 제41조에 따른 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

- 국가안보, 외교상 비밀 등 국가의 중대한 이익이나 범죄수사 등 공익 달성을 위한 개인정보파일은 이를 공개하지 않는 것이 보다 공익에 부합할 수 있다. 따라서 이러한 개인정보파일은 등록·공개 의무를 면제할 수 있다.(「개인정보 보호법」 제32조 제2항의 적용 예외사항 참조) 〈개인정보 보호법령 및 지침 · 고시 해설서〉

등록면제 개인정보 파일
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 사용 되는 개인정보파일 5. 다른 법령에 따라 비밀로 분류된 개인정보파일

등록면제 개인정보 파일 예시
● 공공기관 내부 업무처리를 위한 개인정보 파일 - 임직원 전화번호부, 비상연락망, 인사기록파일 등 - 요금정산, 회의참석자 수당지급, 자문기구운영 등을 위한 개인정보파일 ● 다른 법령에 따른 비밀 개인정보파일 예시 - 「공공기록물관리에 관한 법률」 제33조(비밀 기록물의 관리) - 「보안업무규정」 제4조(비밀의 구분)

● 다음의 경우
- 헌법기관의 개인정보파일(제32조제6항, 표준지침 제54조제1호)
- 법 제58조제1항에 따라 적용이 제외되는 개인정보파일
  ① 공공기관이 처리하는 개인정보 중「통계법」에 따라 수집되는 개인정보파일
  ② 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
  ③ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
- 그 외에 등록 의무가 적용 제외되는 개인정보파일
  ① CCTV 개인영상정보 파일
  ② 자료, 물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위해 운용하는 경우로서, 저장하거나 기록하지 않고 폐기할 목적으로 수집한 개인정보파일 등

● 개인정보처리자는 주기적(1년 1회 이상)으로 개인정보파일의 변경 여부를 확인한 후 변경된 내역을 개인정보보호 종합지원시스템(intra.privacy.go.kr)의 개인정보파일 내용을 변경하고, 개인정보파일대장에도 반영할 것을 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
2.2.2	대상시스템에서 개인정보파일을 신규로 보유하거나 기존 파일을 변경하는 경우, 보호위원회에 등록하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 개인정보파일 58개를 개인정보파일대장에 '업무목적, 보유목적, 보유근거(관련법령), 수집방법, 개인정보 항목, 사용 부서' 등의 항목으로 관리하고 있으나 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 57개 파일만 등록이 되어 있고 최근에 신규 생성된 '○○○파일'은 등록이 누락되어 있음.				

개인정보 파일대장

개인정보파일명	○○○ 파일		
1. 업무분야		2. 단위업무	공식한정통계
3. 보유목적			
4. 보유근거(관련법령)		국가승인통계 승인번호 제118006호]	
5. 수집방법			
6. 대상개인원래			
7. 대상인원수		8. 보유기간 (비고)	영구
9. 기록항목	이름, 전화, 주소		
10. 사용부서			
11. 열람예정일			
12. 열람청구부서 및 주소			
13. 열람제한 (1)열람제한항목	모든항목		
(2)열람제한사유	법률의한 제한(통계법)		
14. 이용, 제공기관명	없음	15. 이용, 제공근거	없음
16. 이용, 제공항목	없음		

개인정보파일 등록 현황

개인정보 열람등요구 안내 | 개인정보파일 목록 검색 | 개인정보 열람등요구 | 개인정보 열람등요구 처리조회

• 기관명 △ △ △ • 파일명 검색 초기화

엑셀받기

번호	기관명	업무분야	파일명
57	△ △ △	OO 업무	공급업체 명단
56	△ △ △	XX 업무	회원 명단
55	△ △ △	□△업무	교육생 명단
54	△ △ △	□△업무	이벤트 참여자 파일

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다.

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

【개인정보 보호법 시행령】

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 보호위원회가 정하여 고시하는 바에 따라 보호위원회에 법 제32조제1항 및 이 영 제33조에 따른 등록사항(이하 "등록사항"이라 한다)의 등록을 신청하여야 한다. 등록 후 등록한 사항이 변경된 경우에도 또한 같다.

【표준 개인정보 보호지침】

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다.

② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하여야 한다.

③ 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다.

④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 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 각호와 같다. 신청은 「개인정보 보호법 고시」 이하 "고시"라 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 처리방법
7. 개인정보의 보유기간
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 고시 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 보호위원회에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육과학기술부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육과학기술부의 확인을 받아 보호위원회에 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 보호위원회에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제32조

3 개인정보 처리방침

세부분야	개인정보 처리방침의 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.3.1	● **개인정보 처리방침을 수립하고 인터넷 홈페이지·관보 등에 안내하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 대상시스템의 개인정보 처리방침을 수립하여 안내하고 있으나, "개인정보 처리방침" 이라는 명칭이 아니거나 정보주체가 쉽게 확인할 수 있도록 게시되어 있지 않은 경우				
평가근거 및 의견	● △△△ 기관은 대상시스템(웹 서비스)에 개인정보처리방침을 게시하고 있으나, 그 명칭이 "개인정보처리방침"이 아닌 "개인정보보호정책"으로 되어 있음				

주요 점검 사항

1. 개인정보처리자는 처리하는 개인정보파일에 대하여 개인정보 처리방침을 정하여 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 게재하여야 한다. 다만, 인터넷 홈페이지에 게재할 수 없는 경우 아래에서 제시된 어느 하나 이상으로 방법으로 공개하여야 한다.
   - 개인정보처리자의 사업장 등의 보기 쉬운 장소에 게시하는 방법
   - 관보(공공기관인 경우)나 개인정보처리자의 사업장 등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷 신문에 싣는 방법
   - 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
   - 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법
2. 개인정보처리방침은 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 해야 한다.
3. 개인정보처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.
4. 영업 양도, 합병 등에 따라 개인정보가 이전되는 경우 정보주체에게 이전 사실, 이전 받는 자, 이전을 원하지 아니할 때 조치할 수 있는 방법·절차 등에 관한 정보를 통지하여야 한다.

지표 해설

- 개인정보 처리방침이란 기관에서 보유하고 있는 개인정보파일에 대한 기관의 처리방침에 대한 사항으로 개인정보처리자는 개인정보 처리방침을 수립하여 인터넷 홈페이지 또는 관보 등에 게재하여 정보주체가 쉽게 찾아볼 수 있도록 공개하여야 한다.

- 개인정보 처리방침은 정보주체가 쉽게 확인할 수 있도록 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하여야 하나 인터넷 홈페이지에 게재할 수 없는 경우에는 다음과 같은 방법으로 공개할 수 있다.
  - 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
  - 관보나 개인정보처리자의 사업장 등이 있는 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 및 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
  - 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물 · 소식지 · 홍보지 또는 청구서 등에 지속적으로 싣는 방법(발행될 때마다 계속하여 게재하여야 함)
  - 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

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

- 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.

- 「신용정보법」에서는 신용정보 업무처리와 관련하여 금융위원회가 정하는 '내부관리 규정'을 마련하여 기록을 보존하도록 하고 있으나, 「개인정보 보호법」상 '개인정보 처리방침'과는 내용이 상이하므로, 「개인정보 보호법」에 따른 개인정보 처리방침을 작성하여야 한다.

- 영업의 양도·합병 등으로 개인정보를 다른 사람에게 이전하거나 이전 받는 경우에는 「개인정보 보호법」 제27조에 따라 관련 사항을 정보주체에게 통지하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
2.3.1	개인정보 처리방침을 수립하고 인터넷 홈페이지·관보 등에 안내하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 홈페이지에 개인정보처리방침을 게시하고 있으나, 그 명칭이 "개인정보처리방침"이 아닌 "개인정보보호정책"으로 되어 있으며, 글자크기, 색상 등을 통해 다른 고지사항과 구분하여 정보주체가 쉽게 확인할 수 있도록 게시되어 있지 않음 				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

제30조(개인정보 처리방침의 수립 및 공개) ② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

【개인정보 보호법 시행령】

제31조(개인정보 처리방침의 내용 및 공개방법 등) 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

【표준 개인정보 보호지침】

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지를 통해 지속적으로 개제하여야 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 시행령 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 시행령 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제36조(영상정보처리기기 운영·관리지침) 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제30조

세부분야	개인정보 처리방침의 작성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
2.3.2	● **개인정보 처리방침은 법률 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보 처리방침을 수립하여 인터넷 홈페이지, 관보 등에 안내하고 있으나, 내용이 법적 요건의 일부만을 포함하고 있거나, 일부 내용이 미흡한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 홈페이지의 개인정보처리방침에 개인정보의 처리목적, 개인정보 파일 현황 등 법적 필수사항 대부분을 포함하고 있으나 '개인정보의 안전성 확보조치에 관한 사항'을 누락하고 있음				

주요 점검 사항

1. 개인정보처리방침은 법률 등에서 규정한 내용을 모두 포함하고 있어야 한다.
   ① 개인정보의 처리 목적
   ② 개인정보의 처리 및 보유기간
   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 처리하는 개인정보의 항목
   ⑦ 개인정보의 파기에 관한 사항
   ⑧ 개인정보 보호책임자 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
   ⑨ 개인정보 처리방침의 변경에 관한 사항
   ⑩ 개인정보 보호법 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
   ⑪ 개인정보파일 현황(공공기관의 경우)
   ⑫ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에 한한다.)
   ⑬ 법 제15조제3항과 제17조제4항에 따라 정보주체의 동의없이 추가적인 이용 또는 제공을 할 때 시행령 제14조의2 제1항의 각 호의 고려사항에 대한 판단기준(해당하는 경우에 한한다.)
   ⑭ 가명정보 처리 시 가명정보 처리에 관한 사항(해당하는 경우에 한한다.)
2. 개인정보의 처리 목적, 처리하는 개인정보의 항목 등 개인정보처리방침에 공개된 내용은 오류 및 누락 사항이 없어야 하며, 정보주체가 쉽게 이해할 수 있도록 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

지표 해설

- 개인정보처리자는 개인정보 처리방침에 아래의 개인정보 처리(수집·저장, 이용·제공, 파기)에 대한 사항 등을 포함하여야 한다.

개인정보 처리방침 기재사항
[필수적 기재사항] 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 보호책임자 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처 9. 개인정보 처리방침의 변경에 관한 사항 10. 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항 11. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에 한한다.) **[임의적 기재사항]** 1. 정보주체의 권익침해에 대한 구제방법 2. 개인정보의 열람청구를 접수·처리하는 부서

- 개인정보 최소수집 의무를 명확히 하기 위하여, 개인정보 처리방침에서 명시하는 개인정보 항목이 개인정보의 처리 목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다.
- 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 못하도록 규정하고 있는데, 동 규정에 따라 개인정보주체를 효과적으로 보호하기 위하여 개인정보처리자가 목적에 필요한 최소한의 개인정보 이외에 개인별 맞춤서비스 등을 위하여 처리하는 개인정보의 항목이 있는 경우에는 개인정보주체가 혼동하지 않도록 양자를 구별하여 표시하여야 한다.
- 개인정보처리자는 개인정보 처리방침에 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)을 포함하여야 한다.

개인정보처리방침에 안내하는 개인정보의 제3자 제공에 관한 사항(예시)
가. 제공받는 자 나. 개인정보 제공 목적 다. 제공되는 개인정보 항목 라. 이용 기간 마. 제공 근거(○○법 ○조 혹은 정보주체 동의) *※권고 항목*

- 개인정보처리자는 개인정보 처리방침에 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)을 포함하여야 한다.

개인정보처리방침에 안내하는 위탁에 관한 사항(예시)
가. 수탁자명 나. 위탁하는 업무의 내용 다. 위탁시 처리되는 개인정보 항목 *※권고 항목* 라. 위탁 기간(개인정보 위탁 기간) *※권고 항목*

- 개인정보처리자는 개인정보 처리방침에 정보주체와 법적대리인의 권리·의무 및 그 행사방법에 관한 사항을 포함하여야 한다.
  - 개인정보의 처리에 관한 정보를 제공받을 권리
  - 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
  - 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다)을 요구할 권리
  - 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
  - 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리 등
- 개인정보처리자는 개인정보 처리방침에 개인정보의 안전성 확보조치에 관한 사항을 포함하여야 한다.

개인정보처리방침에 안내하는 안전성확보 조치에 관한 사항
가. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행 나. 개인정보에 대한 접근통제 및 접근 권한의 제한 조치 다. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 라. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치 마. 개인정보에 대한 보안프로그램의 설치 및 갱신 바. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금 장치의 설치 등 물리적 조치 등

- 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리할 것을 권장한다.
- 또한, 개인정보처리방침의 개인정보파일 보유현황 및 파기현황은 기관에서 관리하는 개인정보파일대장과 보호위원회에 등록된 개인정보파일 현황과 일관성을 유지할 것을 권장한다.

개인정보처리방침에 안내하는 개인정보파일 현황(예시)

[개인정보파일 보유 현황]

가. 개인정보파일 명칭
나. 처리목적
다. 개인정보 항목
라. 보유기간
마. 보유 근거(OO법 O조 혹은 정보주체 동의)

[개인정보파일 파기 현황]

가. 개인정보파일 명칭
나. 개인정보 항목
다. 보유기간
라. 파기방법(선택 사항)
마. 파기일자

개인정보 처리방침 작성 예시

○○○부 개인정보 처리방침

○○○부는 개인정보 보호법 제30조에 따라 정보주체의 개인정보를 보호하고 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 하기 위하여 다음과 같이 개인정보 처리지침을 수립하여 공개합니다.

제1조(개인정보의 처리목적)

① ○○○부는 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, 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 ○○○부가 개인정보 보호법 제32조에 따라 등록·공개하는 개인정보파일의 처리목적은 다음과 같습니다.

순번	개인정보파일의 명칭	운영근거/처리목적	개인정보파일에 기록되는 개인정보의 항목	보유 기간
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, 주민등록번호, 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 개인정보보호위원회 개인정보보호 포털 (www.privacy.go.kr) →민원마당→개인정보 열람등요구→개인정보파일 목록검색 메뉴를 활용해주시기 바랍니다.

제2조(개인정보의 처리 및 보유기간)

① ○○○부는 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 보유합니다. 다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지 보유합니다.
   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. 민원사무 처리 : 민원처리 종료 후 3년
3. 「○○에 관한 법률」 제0조에 따른 개인정보 처리·보유 : ○○년

제3조(개인정보의 제3자 제공)

① ○○○부는 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 ○○○부는 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 : 〈○○시까지〉 또는 〈○년〉

제4조(개인정보처리의 위탁)

① ○○○부는 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

〈전화 상담센터 운영〉

- 위탁받는 자 (수탁자) : ○○○ 컨택센터
- 위탁하는 업무의 내용 : 전화상담 응대, 부서 및 직원 안내

② ○○○부는 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(정보주체와 법정대리인의 권리·의무 및 행사방법)

① 정보주체와 법정대리인은 ○○○부에 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 ○○○부에 대해 서면, 전화, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며 ○○○부는 이에 대해 지체없이 조치하겠습니다.

③ 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 ○○○부는 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 처리 방법에 관한 고시」 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.
⑤ 정보주체는 개인정보 보호법 등 관계법령을 위반하여 ○○○부가 처리하고 있는 정보주체 본인이나 타인의 개인정보 및 사생활을 침해하여서는 아니됩니다.

제6조(처리하는 개인정보 항목) ○○○부는 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, 생년월일 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 ○○○부는 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기합니다.
② 정보주체로부터 동의 받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보(또는 개인정보파일)을 별도의 데이터베이스(DB)로 옮기거나 보관 장소를 달리하여 보존합니다.
③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차
   ○○○부는 파기하여야 하는 개인정보(또는 개인정보파일)에 대해 개인정보 파기계획을 수립하여 파기합니다. ○○○부는 파기 사유가 발생한 개인정보(또는 개인정보파일)을 선정하고, ○○○부는 개인정보 보호책임자의 승인을 받아 개인정보(또는 개인정보파일)을 파기합니다.
2. 파기방법
   ○○○부는 전자적 파일 형태로 기록·저장된 개인정보는 기록을 재생할 수 없도록 로우레밸포맷(Low Level Format) 등의 방법을 이용하여 파기하며, 종이 문서에 기록·저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

제8조(개인정보의 안전성 확보조치) ○○○부는 개인정보의 안전성 확보를 위해 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치 : 내부 관리계획 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 ○○○부는 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호책임자

성명 : ○○○

직책 : ○○○ 실장

직급 : ○급

연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

※ 개인정보 보호 담당부서로 연결됩니다.

▶ 개인정보 보호 담당부서

부서명 : ○○○

담당자 : ○○○

연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

② 정보주체께서는 ○○○부의 서비스(또는 사업)을 이용하시면서 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의하실 수 있습니다. ○○○부는 정보주체의 문의에 대해 지체 없이 답변 및 처리해드릴 것입니다.

제10조(개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항)

1. 쿠키의 사용 목적

① ○○○부는 개인 맞춤 서비스를 제공하기 위해서 이용자에 대한 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다. 쿠키는 웹사이트 서버가 이용자의 브라우저에게 전송하는 소량의 정보로서 이용자 컴퓨터의 하드디스크에 저장됩니다.

② ○○○부는 쿠키의 사용을 통해서만 가능한 특정된 맞춤형 서비스를 제공할 수 있습니다.

③ ○○○부는 회원을 식별하고 회원의 로그인 상태를 유지하기 위해 쿠키를 사용할 수 있습니다.

2. 쿠키의 설치/운용 및 거부

① 이용자는 쿠키 설치에 대한 선택권을 가지고 있습니다. 따라서 이용자는 웹브라우저에서 옵션을 조정함으로써 모든 쿠키를 허용/거부하거나, 쿠키가 저장될 때마다 확인을 거치도록 할 수 있습니다.

- 쿠키 설치 허용 여부를 지정하는 방법(Internet Explorer의 경우)은 다음과 같습니다.

[도구] 메뉴에서 [인터넷 옵션]을 선택합니다.

[개인정보 탭]을 클릭합니다.

[개인정보취급 수준]을 설정하시면 됩니다.

② 쿠키의 저장을 거부할 경우에는 개인 맞춤서비스 등 ○○○부가 제공하는 일부 서비스는 이용이 어려울 수 있습니다.

제11조(개인정보 열람청구)

① 정보주체는 개인정보 보호법 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. ○○○부는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

▶ 개인정보 열람청구 접수·처리 부서
부서명 : ○○○
담당자 : ○○○
연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

② 정보주체께서는 제1항의 열람청구 접수·처리부서 이외에, 개인정보보호위원회의 '개인정보보호 포털' 웹사이트(www.privacy.go.kr)를 통하여서도 개인정보 열람청구를 하실 수 있습니다.

▶ 개인정보보호위원회 개인정보보호 포털 → 민원마당 → 개인정보 열람등 요구 (공공아이핀을 통한 실명인증 필요)

제12조(권익침해 구제방법) 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의하실 수 있습니다.

〈아래의 기관은 ○○○부와는 별개의 기관으로서, ○○○부의 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 : (05717) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터

▶ 개인정보 분쟁조정위원회
- 소관업무 : 개인정보 분쟁조정신청, 집단분쟁조정 (민사적 해결)
- 홈페이지 : kopico.go.kr
- 전화 : (국번없이) 1833-6972
- 주소 : (03171) 서울시 종로구 세종대로 209, 정부서울청사 12층 개인정보 분쟁조정위원회

▶ 대검찰청 사이버범죄수사단 : 02-3480-3573 (www.spo.go.kr)

▶ 경찰청 사이버테러 대응센터 : 1566-0112 (www.netan.go.kr)

제13조(영상정보처리기기 설치·운영)

① ○○○부는 아래와 같이 영상정보처리기기를 설치·운영하고 있습니다.

1. 영상정보처리기기 설치근거·목적 : ○○○부의 시설안전 및 화재예방
2. 설치 대수, 설치 위치, 촬영 범위 : 청사 로비·민원실 등 주요시설물을 촬영범위로 ○○대 설치
3. 관리책임자, 담당부서 및 영상정보에 대한 접근권한자 : ○○○ 과 ○○○ 과장
4. 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
   - 촬영시간 : 24시간 촬영
   - 보관기간 : 촬영 시부터 30일
   - 보관장소 및 처리방법 : ○○○과 영상정보처리기기 통제실에 보관·처리
5. 영상정보 확인 방법 및 장소 : 관리책임자에 요구 (○○○과)
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 : 내부 관리계획 수립, 접근통제 및 접근권한 제한, 영상정보의 안전한 저장·전송기술 적용, 처리기록 보관 및 위·변조 방지조치, 보관시설 마련 및 잠금장치 설치 등

제14조(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)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
2.3.2	개인정보 처리방침은 법률 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 홈페이지의 개인정보 처리방침 중 '제3조 개인정보 처리위탁에 관한 사항' 항목에 개인정보처리의 위탁에 관한 사항을 반영하고 있으나 (주)○○○ 업체만 안내하고 있고 위탁업체인 XXX업체는 누락되어 있음.				

개인정보 처리방침 (위탁에 관한 사항)	**제3조 개인정보 처리 위탁에 관한 사항** △ △ △ 는 개인정보의 처리업무를 위탁하는 경우 다음의 내용이 포함된 문서에 의하여 처리하고 있습니다. 가. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 나. 개인정보의 관리적·기술적 보호조치에 관한 사항 다. 개인정보의 안전관리에 관한 사항 위탁업무의 목적 및 범위, 재위탁 제한에 관한 사항, 개인정보 안전성 확보 조치에 관한 사항, 위탁업무와 관련하여 보유하고 있는 개인정보의 관리현황점검 등 감독에 관한 사항, 수탁자가 준수하여야할 의무를 위반한 경우의 손해배상책임에 관한 사항 또한, 위탁하는 업무의 내용과 개인정보 처리업무를 위탁받아 처리하는 자("수탁자")에 대하여 해당 홈페이지에 공개하고 있습니다. 수탁기관명 : (주) ○○○ - 위탁업무내용 : 홈페이지 운영 및 유지보수 - 위탁기간 : 계약완료일

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호 업무 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 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

【개인정보 보호법 시행령】

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

【표준 개인정보 보호지침】

제4조(개인정보 보호원칙) ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.

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 명확하게 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(해당되는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당되는 경우에만 정한다)
7. 시행령 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.

제36조(영상정보처리기기 운영·관리지침) 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.

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제30조
- 개인정보 처리방침 작성예시 – 공공기관용/민간용/소상공인용 (개인정보보호 종합포털->자료실 참고)

3. 개인정보 처리단계별 보호조치

1 수집

세부분야	개인정보 수집의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.1	● **개인정보를 수집하는 경우 법령에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보 수집 시 일부 평가업무에서 법적인 근거가 없으며, 정보주체의 동의를 받지 않은 경우				
평가근거 및 의견	● ○○기관에서 제공하는 ○○서비스를 이용하는 고객들의 관리를 위해 개인정보를 수집하고 있으나 일부 평가업무에서 수집하는 개인정보에 대한 법적인 근거가 없으며, 별도의 정보주체 동의를 받지 않음				

주요 점검 사항

1. 개인정보의 수집 시 아래와 같이 적법한 근거가 있어야 한다.
   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 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. 정보주체의 동의를 받는 경우에는 관련 사항을 모두 알려야 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

3. 정보주체의 동의 여부, 동의 일시 등을 사후에 확인할 수 있도록 개인정보처리시스템에 관련 내용이 기록되어야 한다.

4. SNS, 인터넷 홈페이지 등 공개된 매체 및 장소에서 개인정보를 수집하는 경우에는 정보주체의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하여야 한다.

※ 개인정보 흐름분석 결과를 바탕으로 모든 평가업무별 수집 흐름별로 점검 필요

지표 해설

- 본 지표에서는 개인정보 흐름도 등 개인정보 흐름분석 결과를 바탕으로 각 개인정보 수집 경로 및 흐름별로 개인정보 수집의 근거가 적절한지 평가한다. 개인정보를 수집하는 경로가 평가 업무별로 상이하거나 온라인, 오프라인 등 다양하게 존재한다면 해당 경로 상의 모든 개인정보 수집절차가 적절한지 빠짐없이 확인하여야 한다.
- 개인정보처리자는 다음 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있다.

① 정보주체의 동의

개인정보처리자는 정보주체의 동의를 받은 경우에 개인정보를 수집할 수 있는데, '동의'는 개인정보처리자가 개인정보를 수집 · 이용하는 것에 대한 정보주체의 자발적인 승낙의 의사표시로서(서명날인, 구두, 홈페이지 동의 등) 동의여부를 명확하게 확인할 수 있어야 한다.

정보주체는 서비스를 제공받기 위하여 가입신청서 등의 서면에 직접 자신의 성명을 기재하고 인장을 찍는 방법 또는 자필 서명하거나, 인터넷 웹사이트 화면에서 '동의', '동의안함' 버튼을 클릭하는 등으로 동의의 의사표시를 할 수 있다.

개인정보 수집·이용 동의시 고지 사항
1. 개인정보의 수집·이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우 그 불이익의 내용

동의 사례
1. 영화관 멤버십카드 발급시 개인정보 활용동의서에 기명날인하는 경우 2. 공공기관의 인터넷홈페이지 회원가입시 개인정보 수집·이용 동의에 체크하는 경우

개인정보 수집동의 획득 예시
[수집하는 개인정보의 항목] [개인정보 수집 목적] [개인정보 보유기간] [개인정보 수집 동의 거부의 권리]
개인정보의 수집 및 이용목적에 동의하십니까? ☐ 동의함 ☐ 동의하지 않음

② 법률규정이 있거나 법령상 의무준수를 위해 불가피한 경우

'법률의 특별한 규정'이란 법률에서 개인정보의 수집·이용을 구체적으로 요구하거나 허용하고 있어야 한다. 수집·이용할 수 있는 개인정보의 대상·범위가 막연한 경우는 특별한 규정이라고 할 수 없다. 법률에 특별한 규정이 있어야 하므로 시행령이나 시행규칙에 규정하는 것은 안 된다.

'법률의 특별한 규정' 예시	
「신용정보법」	**제40조(신용정보회사등의 금지사항)** ① 신용정보회사등은 다음 각 호의 행위를 하여서는 아니 된다. 4. 특정인의 소재 및 연락처(이하 "소재등"이라 한다)를 알아내는 행위. 다만, 채권추심회사가 그 업무를 하기 위하여 특정인의 소재등을 알아내는 경우 또는 다른 법령에 따라 특정인의 소재등을 알아내는 것이 허용되는 경우에는 그러하지 아니하다.
「보험업법」	**제176조 (보험요율산출기관)** ⑩ 보험요율 산출기관은 순보험요율을 산출하기 위하여 필요한 경우 또는 보험회사의 보험금 지급업무에 필요한 경우에는 음주운전 등 교통법규 위반 또는 운전면허(「건설기계관리법」 제26조제1항 본문에 따른 건설기계조종사면허를 포함한다. 이하 제177조에서 같다)의 효력에 관한 개인정보를 보유하고 있는 기관의 장으로부터 그 정보를 제공받아 보험회사가 보험계약자에게 적용할 순보험료의 산출 또는 보험금 지급 업무에 이용하게 할 수 있다.
「자동차 손해배상 보장법」	**제14조 (진료기록의 열람 등)** ① 보험회사등은 의료기관으로부터 제12조제2항에 따라 자동차보험진료수가를 청구받으면 그 의료기관에 대하여 관계 진료기록의 열람을 청구할 수 있다. ② 제12조의2에 따라 심사 등을 위탁받은 전문심사기관은 심사 등에 필요한 자료를 의료기관에 요청할 수 있다. ③ 제1항 또는 제2항의 경우 의료기관은 정당한 사유가 없으면 이에 따라야 한다.
「병역법」	**제11조의2(자료의 제출 요구 등)** ① 지방병무청장은 징병검사와 관련하여 징병검사전담의사, 징병검사전문의사(徵兵檢査專門醫師) 또는 제12조의2에 따라 신체검사를 위하여 파견된 군의관(軍醫官) 등이 질병이나 심신장애의 확인을 위하여 필요하다고 인정하는 경우 「의료법」에 따른 의료기관의 장, 「국민건강보험법」에 따른 국민건강 보험공단의 장, 「초·중등교육법」에 따른 학교의 장 등에 대하여 징병검사 대상자의 진료기록·치료 관련 기록 내역, 학교생활기록부 등의 제출을 요구할 수 있다. 이 경우 자료 제출을 요구받은 사람은 특별한 사유가 없으면 요구에 따라야 한다. ② 누구든지 제1항에 따라 취득한 징병검사 대상자에 대한 정보·자료를 공개 또는 누설하거나 다른 사람에게 제공하는 등 징병검사 외의 목적으로 사용하여서는 아니 된다.
「의료법」	**제21조의2(진료기록의 송부 등)** ① 의료인 또는 의료기관의 장은 다른 의료인 또는 의료기관의 장으로부터 제22조 또는 제23조에 따른 진료기록의 내용 확인이나 진료기록의 사본 및 환자의 진료경과에 대한 소견 등을 송부 또는 전송할 것을 요청받은 경우 해당 환자나 환자 보호자의 동의를 받아 그 요청에 응하여야 한다. 다만, 해당 환자의 의식이 없거나 응급환자인 경우 또는 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 환자 보호자의 동의 없이 송부 또는 전송할 수 있다.

	제22조(진료기록부등) 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. ②의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자의무기록(電子醫務記錄)을 포함하며, 추가기재 · 수정된 경우 추가기재 · 수정된 진료기록부등 및 추가기재 · 수정 전의 원본을 모두 포함한다. 이하 같다]을 보건복지부령으로 정하는 바에 따라 보존하여야 한다.

'법령상 의무준수'란 법령에서 개인정보처리자에게 일정한 의무를 부과하고 있는 경우로서 해당 개인정보처리자가 그 의무 이행을 위해서 개인정보를 불가피하게 수집·이용할 수 밖에 없는 경우를 말한다. 법률에 의한 의무뿐만 아니라 시행령, 시행규칙에 따른 의무도 포함된다.

'불가피한 경우'란 개인정보를 수집하지 않고는 법령에서 부과하는 의무를 이행하는 것이 불가능하거나 개인정보처리자가 다른 방법을 사용하여 의무를 이행하는 것이 현저히 곤란한 경우를 의미한다.

법령에 따라 연령 확인이 필요한 경우
● 「청소년보호법」 제16조 : 청소년 유해매체물 판매, 대여, 배포 등을 하고자 하는 경우 그 상대방의 연령을 확인하여야 함 ● 「청소년보호법」 제26조 : 인터넷게임(정보통신망을 통하여 실시간으로 제공되는 게임물)의 제공자는 16세 미만 청소년에게 오전0시~오전6시까지 인터넷게임을 제공해서는 안됨 ● 「청소년보호법」 제29조 : 청소년유해업소 업주는 종업원을 고용하고자 하는 때 그 연령을 확인해야 하며, 출입자의 연령을 확인하여 청소년이 당해 업소에 출입·이용하지 못하게 해야 함 ● 민법 상 미성년자 보호제도 : 우리나라 법원은 미성년자의 적극적인 기망행위만을 「사술」로 인정하고 사술의 존재에 대하여 이를 주장하는 상대방이 입증하여야 한다고 판시하고 있음, 따라서 미성년자와 거래를 하는 사업자는 미성년자인지 여부를 신분증 확인과 같은 보다 적극적인 수단에 따라 확인하여야 할 필요가 있음

법령에 따라 본인 확인이 필요한 경우
● 정보통신망법 제44조의5 : 게시판이용자의 본인확인 ● 공직선거법 제82조의6 : 인터넷언론사 게시판·대화방 등의 실명확인 ● 금융실명거래 및 비밀보장에 관한 법률 제3조 : 금융실명거래를 위한 실명확인 ● 법원경비관리대의 설치, 조직 및 분장사무 등에 관한 규칙. 제5조 : 법원경비관리대원은 주민등록증 또는 그 밖의 신분을 확인할 수 있는 자료에 의하여 청사출입자의 신분을 확인하여야 함 ● 선원법에 따른 신원조사 ● 그 밖에 공공기관이 접수된 민원을 처리하기 위하여 신고자를 확인하는 경우

법령상 보험자의 의무 이행
● 책임보험계약의 보험자는 피보험자가 보험기간 중의 사고로 인하여 제3자에게 배상할 책임을 진 경우에 보상 책임 의무가 있다(「상법」 제719조). 따라서 보험계약상 보상 책임 의무를 이행하기 위하여 불가피한 경우 정보 주체의 동의없이 개인정보 수집·이용이 가능하다.

③ 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우

공공기관은 개인정보를 수집할 수 있도록 명시적으로 허용하는 법률 규정이 없더라도 법령 등에서 소관 업무를 정하고 있고 그 소관 업무의 수행을 위하여 불가피하게 개인정보를 수집할 수밖에 없는 경우에는 정보주체의 동의없이 개인정보 수집이 허용된다. 사실 '법령 등에서 정하는 소관업무 수행'은 '법령상 의무준수'에 포함된다고 볼 수도 있으나, 법령상 의무준수와 소관업무 수행의 차이를 좀 더 명확하게 하기 위하여 별도로 규정한 것이다.

'법령 등에서 정하는 소관업무'란 「정부조직법」 및 각 기관별 직제령·직제규칙, 개별 조직법 등에서 정하고 있는 소관 사무 이외에, 「주민등록법」, 「국세기본법」, 「의료법」, 「국민건강보험법」 등 소관법령에 의해서 부여된 권한과 의무, 지방자치 단체의 경우 조례에서 정하고 있는 업무 등을 의미한다.

'불가피한 경우'란 개인정보를 수집하지 아니하고는 법령 등에서 해당 공공기관에 부여하고 있는 권한의 행사나 의무의 이행이 불가능하거나 다른 방법을 사용하여 소관 업무를 수행하는 것이 현저히 곤란한 경우를 의미한다.

공공기관의 소관업무 예시
● 인사혁신처가 「정부조직법」 제22조의3, 「인사혁신처와 그 소속기관 직제」 및 「인사혁신처와 그 소속기관 직제 시행규칙」에 따라 공무원의 인사·윤리·복무·연금 등 관리를 위해 공무원인사 관련파일을 수집·이용하 거나 국가인재데이터베이스 시스템을 구축·운영하는 경우 ● 국민건강보험공단이 [국민건강보험법] 제14조에 따라 보험급여관리 등을 위하여 진료내역 등을 수집·이용하는 경우

④ 계약 체결·이행을 위해 불가피하게 필요한 경우

정보주체와 계약 체결 및 이행을 위하여 개인정보의 수집이 불가피하게 수반되는 경우까지 정보주체의 동의를 받도록 하면 경제활동에 막대한 지장을 초래하고 동의획득에 소요되는 비용만 증가시키게 되므로, 계약 체결이나 이행을 위해 불가피하게 필요한 개인정보는 정보주체에 대한 고지 및 동의 없이도 개인정보를 수집할 수 있도록 한 것이다.

'계약체결'에는 계약체결을 위한 준비단계도 포함된다. 예컨대 부동산거래에 있어서 계약체결 전에 해당 부동산의 소유자, 권리관계 등을 미리 조사·확인하는 경우가 이에 해당한다. 단, 계약 미체결시에는 수집한 개인정보는 즉시 파기하여야 한다.

계약체결의 사례
● 보험회사가 계약체결을 위해 청약자의 자동차사고이력, 다른 유사보험의 가입여부등에 관한 정보를 수집하는 경우 ● 거래 체결 전에 거래상대방의 신용도 평가를 위해 정보를 수집·이용하는 경우 ● 회사가 취업지원자와의 근로계약 체결 전에 지원자의 이력서, 졸업증명서, 성적증명서 등 정보를 수집·이용하는 경우

'계약이행'은 물건의 배송·전달이나 서비스의 이행과 같은 주된 의무의 이행 뿐만 아니라 부수의무 즉 경품배달, 포인트(마일리지)관리, 애프터서비스 의무 등의 이행도 포함된다.

계약이행의 사례
● 고객이 주문한 상품을 배송하기 위하여 주소, 연락처 정보를 수집하는 경우 ● 경품행사시 당첨자에게 경품을 발송하기 위해 주소와 연락처 정보를 요구하는 경우 ● 쇼핑몰이 주문시 포인트를 지급하기로 약정하고 주문정보를 수집하는 경우

근로자가 사용자에게 근로를 제공하고 사용자는 이에 대하여 임금을 지급하는 것을 목적으로 근로계약을 체결한 경우, 근로계약을 이행하기 위해서 직원의 개인정보를 수집·이용하는 것은 반드시 필요한 사항이므로 사용자는 근로자의 임금지급, 계약서에 명시된 복지제공 등 근로계약을 이행하기 위하여 근로자의 동의없이 개인정보를 수집·이용할 수 있다.

⑤ 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

1) 의사표시를 할 수 없는 상태

정신미약, 교통사고, 수술(의사표시를 하기 어려운 의료행위 포함) 등으로 정보 주체가 자신의 의사표시를 할 수 없거나, 태풍·홍수·화재 등 재난상태에 고립되어 있거나 납치·감금 등 범죄자들의 수중에 구금되어 있어 정보 주체의 의사를 물어볼 수 없는 경우를 말한다.

2) 사전 동의를 받을 수 없는 경우

주소불명, 전화불통, 이메일차단 등 불가피한 사유로 사전에 동의를 받을 수 없는 경우에 한한다. 수차례 전화를 걸었으나 정보주체 또는 법정대리인이 전화를 받지 아니한 경우에도 전화를 기다릴 시간적 여유가 없다는 사전 동의를 받을 수 없는 경우에 해당한다. 그러나 정보주체 또는 법정대리인이 멀리 떨어져 있어 동의를 받기 어렵다거나 단순히 동의를 거부하고 있다는 사실만으로는 사전 동의를 받을 수 없는 경우에 해당하지 않는다.

사전 동의를 받을 수 없는 급박한 상황이 해소된 경우 개인정보처리자는 사후적으로 정보주체의 승인을 받아야 한다. 개인정보처리자는 정보주체의 사전동의 없이 개인정보를 수집 또는 이용한 경우에도 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집 또는 이용한 사실, 그 사유와 이용내역을 알려야 한다. 급박한 사유가 해소된 이후 계속해서 정보주체의 개인정보를 이용하려는 경우에는 정보주체의 동의를 받아야 한다.

3) 명백히 정보주체 등의 이익을 위한 경우

개인정보의 수집·이용 목적이 명백하게 정보주체 또는 제3자의 생명·신체·재산상의 이익을 위한 것이어야 한다. 이익이 되지만 동시에 손해가 될 수도 있는 경우에는 정보주체의 동의없이 개인정보를 수집할 수 없다.

문제는 제3자에게는 명백히 이익이 되지만 정보주체에게는 손해가 되는 경우이다. 이 경우에는 제3자의 이익이 정보주체의 이익보다 월등한 경우에만 동의없는 개인정보 수집이 가능하다고 하여야 할 것이다. 특히 제3자의 재산상 이익은 정보주체의 생명, 신체상 이익을 앞설 수는 없다고 보아야 한다.

4) 급박한 생명·신체·재산상 이익

생명·신체·재산상 이익이 급박해야 한다. 정보주체 또는 법정대리인의 동의를 받을 수 있는 충분한 시간적 여유가 있거나 다른 수단에 의해서도 생명, 신체, 재산상의 이익을 보호할 수 있다면 급박한 상태에 있다고 할 수 없다.

급박한 이익의 사례
● 조난·홍수 등으로 실종되거나 고립된 사람을 구조하기 위하여 연락처, 주소, 위치정보 등 개인정보를 수집하는 경우 ● 아파트에 화재가 발생한 경우, 집안에 있는 자녀를 구하기 위해 해당 자녀 또는 부모의 이동전화번호를 수집하는 경우 ● 의식불명이나 중태에 빠진 환자의 수술등 의료조치를 위하여 개인정보를 수집 ● 고객이 전화 사기(보이스피싱)에 걸린 것으로 보여 은행이 임시로 자금이체를 중단시키고 고객에게 사실 확인을 하고자 하는 경우

⑥ 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우

개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우에는 정보주체의 동의 없이 개인정보를 수집할 수 있다. 그러나 개인정보처리자의 이익이 명백하게 정보주체의 권리보다 우선하여야 하고, 수집하고자 하는 개인정보가 개인정보처리자의 정당한 이익과 상당한 관련이 있어야 하며 합리적인 범위를 초과해서는 안 된다.

1) 개인정보처리자의 정당한 이익

요금 징수 및 정산, 채권추심, 소 제기 및 진행 등을 위하여 증빙자료를 조사, 확보하는 경우, 영업비밀 유출 및 도난방지, 출입이 통제되고 있는 사업장내 시설안전 등의 목적으로 CCTV 설치 등 계약이나 법률에 기한 개인정보처리자의 정당한 이익이 존재해야 한다.

2) 명백하게 정보주체의 권리보다 우선

개인정보처리자의 정당한 이익을 위한 것이라고 하더라도 정보주체의 사생활을 과도하게 침해하거나 다른 이익을 침범하는 경우에는 정보주체의 동의없이 개인정보를 수집할 수 없다.

정보주체의 권리보다 명백하게 개인정보처리자의 이익이 월등해야 한다. EU에서는 이익형량의 원칙에 따라 정보주체의 이익과 개인정보처리자의 이익을 비교 형량하도록 하고 있으나 우리나라에서는 개인정보처리자의 이익이 명백히 우선하는 경우에만 개인정보 수집이 허용된다.

명백한 판단 사례
● 회사가 업무효율성 및 영업비밀 보호 등을 이유로 직원의 업무처리 내역 및 인터넷 접속내역 등을 모니터링 하는 시스템을 설치하는 것은 정보주체 권리보다 명백히 우선한다고 보기는 어려우므로, 이 경우는 노사 합의에 따라 처리하거나 직원에 대한 고지 또는 동의절차를 거치는 것이 바람직하다.

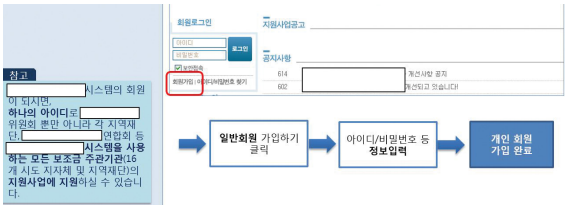
3) 상당한 관련성과 합리적 범위 내의 수집

개인정보처리자의 정당한 이익이 존재하고, 그것이 명백하게 정보주체의 권리보다 우선한다고 하더라도 해당 개인정보가 개인정보처리자의 정당한 이익과 관련성이 낮거나 합리적인 범위를 초과해서는 안 된다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.1	개인정보를 수집하는 경우 법령에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?		○		
평가근거 및 의견	● OO기관은 10개 평가업무 중 3개 평가업무에서 개인정보를 수집하고 있음(AA업무, BB업무, 회원관리업무) ● 3개 업무 중 AA업무와 BB업무는 법률 규정 및 법령 의무준수 등 적절한 수집근거를 보유하고 있음 ● 하지만, 홈페이지 회원관리 업무의 경우 개인정보 수집의 법률적 근거가 없어 개인정보 수집 동의 절차가 필요하지만, 홈페이지 회원가입 화면설계서 상에는 정보주체의 동의를 받기 위한 절차가 반영되어 있지 않음.				

평가업무명	수집근거	분석내용
AA업무	OO법률 제0조	법률에 규정하고 있음
BB업무	OO법률 시행령 제0조	법령상 의무준수를 위해 불가피한 경우
회원관리 업무	정보주체의 동의	정보추체 동의 누락됨

회원가입 화면설계서	

관련법령 및 문서

관련 법령 · 지침

【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.

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

제22조(동의를 받는 방법)

② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

【개인정보 보호법 시행령】

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 법 제22조제2항에서 "대통령령으로 정하는 중요한 내용"이란 다음 각 호의 사항을 말한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 항목의 사항
   가. 제18조에 따른 민감정보
   나. 제19조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호
3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

【표준 개인정보 보호지침】

제6조(개인정보의 수집) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 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 법령에서 부과하는 구체적인 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관업무를 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 개인정보처리자가 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함 등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자가 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를

수집하는 경우, 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지등에 게시하거나 게시하도록 허용한 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 대리인으로부터 또는 의사표시를 하는 경우 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제15조
- 개인정보 수집·제공 동의서 가이드라인(안)

세부분야	개인정보 수집의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.2	● **개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보 수집 목적에 대한 범위와 근거를 명시한 문서가 없거나, 문서에서 명시한 범위와 다르게 수집하고 있는 경우				
평가근거 및 의견	● ○○시스템에서 처리하는 개인정보 수집 목적, 범위, 근거가 기관 내 업무지침에 명시하고 있으나, 화면설계서 및 테이블정의서에는 지침에서 명시한 항목 이외의 추가적인 항목을 수집하고 있음				

주요 점검 사항

1. 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다.
2. 필수로 수집하는 개인정보의 경우 각 항목 별로 해당 개인정보가 최소한의 개인정보라는 입증 근거를 제시할 수 있어야 한다.

지표 해설

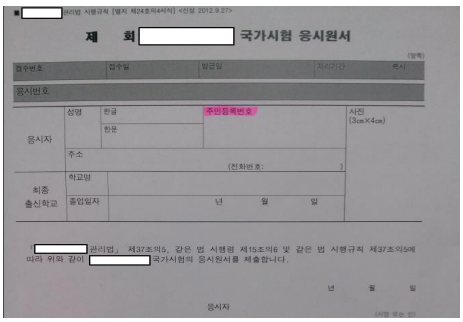
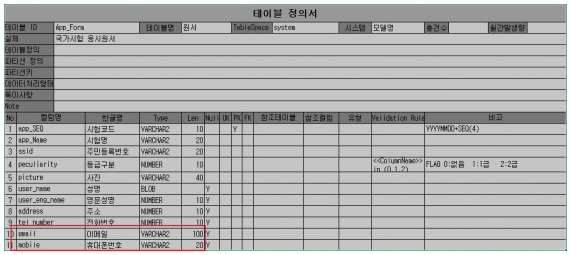
- 본 지표에서는 개인정보 처리 업무표, 개인정보 흐름도 등 개인정보 흐름분석 결과를 바탕으로 각 개인정보 수집 경로 및 흐름별로 업무에 필요한 최소한의 개인정보만 수집하는지의 관점에서 수집항목의 타당성을 평가한다.
- 「개인정보 보호법」 제15조제1항 각 호의 목적을 위해서 정보주체의 개인정보를 수집할 때에는 그 목적에 필요한 범위 내에서 최소한의 개인정보만을 수집하여야 한다.
  정보주체의 동의를 받으면 필요 최소한의 정보 이외의 정보도 수집·이용이 가능하나 필요 최소한의 정보 이외의 정보를 필요 최소한의 정보라고 하여 제공을 의무화하거나 필수적 동의 사항으로 하여 동의를 강요해서는 안 된다.

최소정보의 예
1. 쇼핑업체가 고객에게 상품을 배송하기 위해 수집한 이름, 주소, 전화번호(자택 및 휴대전화번호) 등은 필요 최소한의 개인정보라고 할 수 있으나, 직업, 생년월일 등 배송과 관련 없는 개인정보를 요구하는 것은 최소 정보의 범위를 벗어난 것임 2. 취업 희망자의 경력, 전공, 자격증 등에 관한 정보는 업무능력을 판단하기 위한 최소한의 정보라고 할 수 있으나 가족관계, 결혼유무, 본적(원적) 등에 관한 정보는 최소정보의 범위를 벗어난 것임

- 최소한의 개인정보라는 입증책임은 개인정보처리자가 부담한다. 즉 개인정보처리자가 수집한 개인정보가 최소한의 개인정보라는 것을 입증하지 못하면 개인정보처리자가 패소하게 된다. 만약 필요 최소한 이상으로 개인정보를 수집하고자 하는 경우에는 「개인정보 보호법」 제15조제1항에 따라 정보주체의 동의 없이 개인정보를 수집할 수 있는 경우에도 정보주체의 동의를 받아야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.2	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고 있습니까?			○	
평가근거 및 의견	●○○협회는 ○○법에 의거 국가시험 응시원서를 ○○시스템에서 온라인 신청이 가능하도록 설계하고 있으나, 설계된 문서는 법정서식에 기재된 항목 이외 추가적인 항목을 수집하고 있으며, 관련 항목에 대한 내부검토자료 및 수집목적을 확인할 수 없음.				

법정 신청양식	
테이블 정의서 내용	

제 회 국가시험 응시원서

응시번호

응시자	성명	한글	주민등록번호
		한문	
	주소		
최종 출신학교	학교명		
	졸업일자		년 월 일

사진 (3cm×4cm)

응시자

테이블 정의서

테이블 ID	App_Form	테이블명	원서	TableSpace	system	시스템	모듈명	총건수		실간명생량
설명	국가시험 응시원서									
데이블참의										
파티션 정의										
파티션키										
데이터처리방식										
특이사항										
Note										

No	컬럼명	한글명	Type	Len	Null	UK	PK	FK	참조테이블	참조컬럼	유형	Validation Rule	비고
1	app_SEQ	시험코드	VARCHAR2	10			Y						YYYYMMDD+SEQ(4)
2	app_Name	시험명	VARCHAR2	20									
3	ssid	주민등록번호	VARCHAR2	20									
4	peculiarity	등급구분	NUMBER	10								<<ColumnNose>> in (0,1,2)	FLAG 0:없음 1:1급 2:2급
5	picture	사진	VARCHAR2	40									
6	user_name	성명	BLOB		Y								
7	user_eng_name	영문성명	NUMBER	10	Y								
8	address	주소	NUMBER	10	Y								
9	tel_number	자택번호	NUMBER	10	Y								
10	email	이메일	VARCHAR2	100	Y								
11	mobile	휴대폰번호	VARCHAR2	20	Y								

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제3조(개인정보보호 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.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

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.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제1장 제3조, 제3장 제16조

세부분야	개인정보 수집의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.3	● **주민등록번호는 법적 근거가 있는 경우에 한하여 수집하고 있으며, 인터넷 홈페이지에 대해서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 법에 근거가 없이 주민등록번호를 수집하거나, 온라인 서비스(회원가입) 시 단순 실명확인 목적으로 주민등록번호를 수집하고 있는 경우				
평가근거 및 의견	● ○○홈페이지의 회원가입 시 법에 구체적인 근거가 없이 실명인증만을 위해서 주민등록번호를 수집하고 있음				

주요 점검 사항

1. 주민등록번호 수집 법정주의에 따라 법적 근거가 있는 경우에 한해 주민등록번호를 수집하여야 한다.
   ① 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원 규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
   ② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
2. 법적 근거에 따라 주민등록번호 처리가 가능한 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공해야 한다.

지표 해설

- 본 지표에서는 개인정보 처리 업무표, 개인정보 흐름도 등 개인정보 흐름분석 결과를 바탕으로 주민등록번호의 수집·처리가 존재하는 경우 주민등록번호 처리의 법적 근거, 대체수단 제공 여부 등 타당성을 평가한다.
- 2014년 8월 7일 '주민등록번호 수집 법정주의'의 시행 따라 주민등록번호의 처리가 원칙적으로 금지되었으며, 아래 사유에 해당하는 경우에만 예외적으로 허용이 된다.

주민등록번호의 예외적 처리 허용 사유(개인정보 보호법 제24조의2 제1항)
1. 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호 처리를 요구·허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우 3. 기타 주민등록번호 처리가 불가피한 경우로서 개인정보보호위원회가 고시로 정하는 경우

법률 등에 따라 주민등록번호를 수집·이용할 수 있는 예시
1. 「금융실명거래 및 비밀보장에 관한 법률」 제3조에 주민등록증, 주민등록표등본 등 실지명의 확인 의무가 규정되어 있으므로, 금융(실명)거래를 위해서는 정보주체의 주민등록번호 수집·이용 가능 2. 「국민건강보험법」 등 공적보험 처리, 「근로기준법」 제42조 및 동법 시행령 제22조에 따른 임금대장 작성, 「소득세법」에 따른 소득세 원천징수 등을 위한 주민번호 처리근거 존재하므로, 근로계약 체결 및 관계 법령에서 요구하는 기재사항의 작성을 위해서는 임직원의 주민등록번호 수집·이용 가능 ※ 단, 채용전형 진행단계에는 주민등록번호가 불필요하므로 생년월일 등으로 대체하여야 하며, 최종합격자(입사자)에 한해 주민등록번호 수집·이용 가능

- 주민등록번호 뒷자리를 수집·이용하여 회원의 유일성과 식별성을 확보하는 것은 주민등록번호의 체계를 활용하여 주민등록번호 고유의 특성을 이용하는 것이므로 주민등록번호를 수집·이용하는 경우에 해당한다고 볼 수 있다. 따라서 법률, 대통령령으로 주민등록번호를 수집할 수 있는 구체적 근거가 없다면 주민등록번호의 뒷자리를 수집·이용할 수 없다.
- 법적 근거에 따라 주민등록번호를 수집할 수 있는 경우라 하더라도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.
  - 구두, 서면, 전화, 팩스 등을 통해서 회원을 가입받는 경우에는 주민번호대체수단을 도입하지 않아도 된다.
  - 모바일을 통해 회원가입을 받는 경우에도 주민등록번호 대체수단을 제공하여야 한다.
- 주민등록번호 대체수단으로는 아이핀(i-Pin), 휴대폰본인확인, 공인인증서 등의 방법이 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.3	주민등록번호는 법적 근거가 있는 경우에 한하여 수집하고 있으며, 인터넷 홈페이지에 대해서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○협회 ○○시스템의 회원가입 시 실명인증 절차를 거치며 실명인증 방법으로는 주민등록번호를 사용한 방법을 사용하고 있음 (단, 주민등록번호 수집에 따른 법적인 근거는 없는 것으로 확인됨) 회원가입 동의안내				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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

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

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제24조의2
- 주민등록번호 수집금지 제도 가이드라인(2014)

세부분야	동의받는 방법의 적절성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.4	● **개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보 수집 시 법령에서 정한 개인정보의 처리와 정보주체의 동의에 의해 처리하는 개인정보를 구분하여 동의를 받지 않은 경우				
평가근거 및 의견	● ○○시스템에서 ○○법에 의거 수집하는 개인정보 항목 중 이메일, 전화번호 등 일부 항목에 대해서는 법적인 근거가 없으며, 정보주체의 동의 없이 개인정보를 수집·이용하고 있음				

주요 점검 사항

1. 개인정보 처리에 대하여 정보주체의 동의를 받을 때에는 필수 항목과 선택 항목으로 구분하여야 한다.
2. 필수 항목으로 수집하는 개인정보에 대해서는 필수 정보임을 명백히 입증할 수 있어야 한다.
3. 선택적으로 동의할 수 있는 사항에 대해서는 정보주체가 동의여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 선택적으로 동의할 수 있는 사항 외의 사항과 구분하여 표시하여야 한다.
4. 정보주체가 선택적으로 동의할 수 있는 사항에 동의하지 아니하였다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부해서는 안 된다.
5. 정보주체가 주도적으로 동의 의사를 표시할 수 있도록 동의 양식을 구성하여야 한다. ('동의함'에 Default 체크 금지 등)
6. 동의에 대한 기록(동의 여부, 동의 일시 등)은 사후에 확인이 가능하도록 개인정보처리시스템 등에 기록이 보존되어야 한다.

지표 해설

- 본 지표에서는 개인정보 흐름분석 결과를 바탕으로 대상 업무 또는 서비스에 반드시 필요하지 않은 선택정보를 부가적으로 수집하는 경우 적절하게 동의를 받고 있는지 평가한다.
- 개인정보처리자는 정보주체의 동의가 필요 없는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 정보주체의 동의가 필요 없는 개인정보에는 계약의 체결 및 이행을 위해 필수적인 정보, 법령상 의무준수를 위해 불가피한 정보, 급박한 생명·신체·재산상 이익보호를 위해 필요한 정보, 개인정보처리자의 정당한 이익 달성을 위해 필요한 정보 등이 해당되며, 동의가 필요하지 않다는 입증책임은 개인정보처리자가 부담한다.

- 정보주체의 동의를 요하는 개인정보와 동의가 필요 없는 개인정보로 나뉘어 있는 경우에 개인정보처리자가 전자에 대해서 동의를 얻고자 하는 때에는 후자에 관한 사항도 정보주체에게 알려야 한다. 이는 정보주체가 자신이 처리에 동의한 개인정보에 대해서만 개인정보처리가 이루어지는 것으로 오해하고 개인정보의 처리에 관한 불완전한 정보만을 제공받지 않기 위함이다.
- 정보주체는 개인정보 처리에 대한 동의 여부를 결정하고 선택할 수 있는 권리가 보장되어 있으나, 실제로는 정보주체의 동의가 강제되는 경우가 많아 정보주체의 개인정보자기결정권을 보장하기 위하여 동의 방법을 법률로 구체화한 것이다.
- 정보주체가 선택정보의 처리에 대한 동의(제16조제2항), 직접마케팅에 대한 동의(제22조제4항), 목적 외 이용·제공에 대한 동의(제18조제2항제1호)를 거부하였다는 이유로 개인정보처리자는 재화 또는 본질적인 서비스의 제공을 거부하지 못한다. 또한 개인정보 수집에 동의하지 않는다는 이유로 재화 또는 본질적인 서비스의 제공을 거부하는 것도 금지된다.(제16조제3항) 그러나 합리적인 사유에 근거를 둔 거부는 가능하다.

합리적 사유 사례
● 계열사 고객정보DB를 통합하면서 정보 제공 및 공유에 동의하지 않는다고 서비스 제공을 중단하는 것은 불법이나, 정보 제공 및 공유에 동의한 고객들에 대하여 제공하는 5년간 무료 장기 주차권을 거부한 것은 불법이 아니다. ● 광고메일 수신에 동의하지 않는다고 신용카드 발급 또는 쇼핑몰회원 가입을 거절하는 것은 불법이나, 광고 메일 수신자들에게만 부여하는 포인트나 마일리지를 주는 않는 것은 불법이 아니다. ● 회원 가입을 하지 않으면 물품이나 서비스 구입을 할 수 없게 하는 경우에는 최소수집 원칙 위반이나 회원제로 하지 않으면 물품이나 서비스 판매가 현실적으로 어려운 합리적인 이유가 있다면 위법이 아니다(인터넷뱅킹 등)

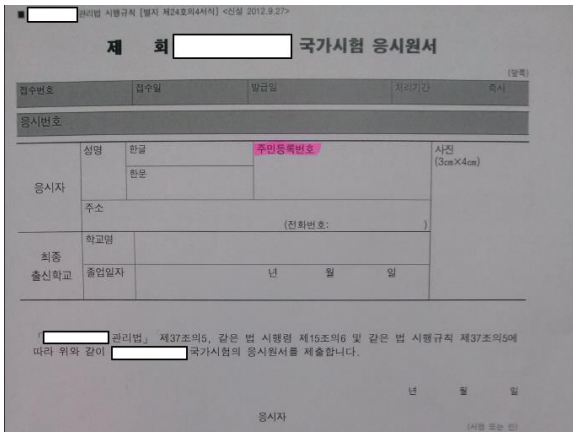
평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.4	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있습니까?			○	

평가근거 및 의견

● ○○협회는 ○○법에 의거 국가시험 응시원서를 ○○시스템에서 온라인 신청이 가능하도록 설계하고 있으며 성명(한글, 한문), 주민등록번호, 사진, 주소, 전화번호, 학교명, 졸업일자, 사진 등은 법정서식에 의한 수집으로 정보주체의 동의 없이 처리할 수 있으나 이메일, 휴대폰번호 등은 정보주체의 동의에 의해 개인정보를 수집하여야 하므로, 구분하여 동의를 받아야 하나, 설계문서에서는 별도 구분 동의를 받도록 설계되어 있지 않음.

법정 신청양식


[redacted]리법 시행규칙 [별지 제24호의4서식] <신설 2012.9.27>

제 회 [redacted] 국가시험 응시원서

(앞쪽)

접수번호	접수일	발급일	처리기간	주사
응시번호				

응시자	성명	한글	주민등록번호	사진 (3cm×4cm)
		한문		
	주소	(전화번호:)		
최종 출신학교	학교명			
	졸업일자	년 월 일		

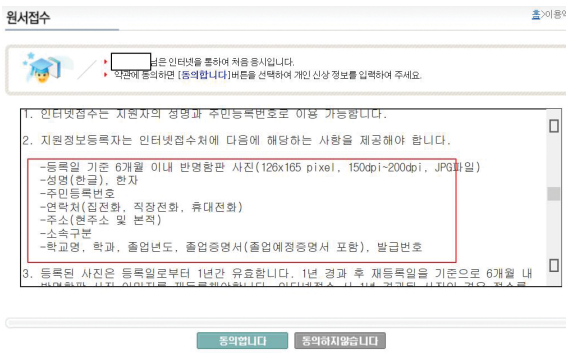
「[redacted]관리법」 제37조의5, 같은 법 시행령 제15조의6 및 같은 법 시행규칙 제37조의5에 따라 위와 같이 [redacted]국가시험의 응시원서를 제출합니다.

년 월 일

응시자

(서명 또는 인)

화면설계


원서접수

홈>이용안

[redacted]분은 인터넷을 통하여 처음 응시입니다.
약관에 동의하면 [동의합니다]버튼을 선택하여 개인 신상 정보를 입력하여 주세요.

1. 인터넷접수는 지원자의 성명과 주민등록번호로 이용 가능합니다.
2. 지원정보등록자는 인터넷접수처에 다음에 해당하는 사항을 제공해야 합니다.
   -등록일 기준 6개월 이내 반명함판 사진(126x165 pixel, 150dpi~200dpi, JPG파일)
   -성명(한글), 한자
   -주민등록번호
   -연락처(집전화, 직장전화, 휴대전화)
   -주소(현주소 및 본적)
   -소속구분
   -학교명, 학과, 졸업년도, 졸업증명서(졸업예정증명서 포함), 발급번호
3. 등록된 사진은 등록일로부터 1년간 유효합니다. 1년 경과 후 재등록일을 기준으로 6개월 내

동의합니다 | 동의하지않습니다

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 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 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

③ 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.

④ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

⑤ 개인정보처리자는 정보주체가 제3항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제4항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑥ 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.

【개인정보 보호법 시행령】

제17조(동의를 받는 방법) ③ 개인정보처리자가 정보주체로부터 법 제18조제2항제1호 및 제22조제4항에 따른 동의를 받거나 법 제22조제3항에 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.

【표준 개인정보 보호지침】

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 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑥ 개개인정보처리자가 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 상호간의 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제22조
- 개인정보 수집·제공 동의서 가이드라인(안)

세부분야	동의받는 방법의 적절성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.5	● **만 14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 만14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받는 내용을 확인할 수 없는 경우				
평가근거 및 의견	● ○○홈페이지는 만 14세 미만 아동도 이용이 가능하며, 회원가입 절차 시 만 14세 미만 아동의 개인정보 수집에 대한 법정대리인의 동의를 받는 절차를 설계문서에서 확인할 수 없음				

주요 점검 사항

1. 만 14세 미만 아동의 개인정보를 처리하기 위하여 동의를 받으려는 경우에는 그 법정대리인의 동의를 받아야 한다.
2. 법정대리인 여부를 확인하는 절차는 정당한 주의의무에 따라 적절히 수행되어야 한다.
3. 법정대리인이 동의를 거부하거나 일정 기간 동의 의사가 확인되지 않은 경우, 지체 없이 관련 개인정보를 파기하여야 한다.
4. 법정대리인 동의에 대한 기록(동의자, 동의 여부, 동의 일시 등)은 사후에 확인이 가능하도록 개인정보처리시스템 등에 기록이 보존되어야 한다.

지표 해설

- 만 14세 미만 아동의 경우 개인정보의 중요성이나 위험성에 대한 인식이 현저히 부족하고, 정보 수집 목적의 진위를 평가하는 능력이 부족하기 때문에 아동을 대상으로 한 무분별한 정보수집을 방지하기 위하여 법정대리인이 미성년자를 대신해서 동의를 하도록 한 것이다.

법정대리인의 정의
● 법정대리인이란 본인의 의사에 의하지 않고 법률의 규정에 의하여 대리인이 된 자로 미성년자의 친권자(「민법」 제909조, 제911조, 제916조, 제920조), 후견인(「민법」 제931조에서 제936조까지), 법원이 선임한 부재자의 재산관리인(「민법」 제22조, 제23조) 등이 이에 해당한다.

- 법정대리인의 동의를 얻기 위해서는 법정대리인의 이름과 연락처를 알아야 하기 때문에 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보(이름과 연락처)는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다. 이 경우 해당 아동에게 자신의 신분과 연락처, 법정 대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다(표준지침 제13조제1항). 또한 아동으로부터 수집한 법정대리인의 개인정보를 동의를 얻기 위한 용도로만 사용해야 하며, 동의에 대한 거부의사가 확인된 경우와 동의여부가 확인되지 아니한 채 5일이 경과한 경우에는 당해 개인정보를 파기하여야 한다.

만 14세 미만 동의획득 예시

Step 1. 어린이 회원 가입(선택)

일반회원	어린이 회원
(만14세 이상의 개인회원)	(만 14세 미만 개인회원)
가입하기	가입하기

Step 2. 보호자 동의

만14세 미만 아동은 회원 가입 시 보호자(법정대리인)의 동의가 있어야 가능합니다. 회원가입 시에는 보호자가 함께 해 주시기 바라며, 보호자는 아래 인증수단 중 하나를 선택해 주시기 바랍니다.

〈휴대폰 인증〉	〈i-PIN 인증〉	〈신용카드〉
보호자 명의의 휴대폰으로 인증하실 수 있습니다.	보호자의 아이핀(i-PIN)으로 인증하실 수 있습니다.	보호자 명의의 신용카드로 인증하실 수 있습니다.
인증하기	인증하기	인증하기

Step 3. 보호자 인증

- 해당 아동의 법정대리인이 맞는지에 대해서는 정당한 주의의무 관점에서 최대한 노력하여야 한다(아동과 법정대리인의 최소 나이 차이 확인, 법정대리인에 대한 본인확인 수단 적용 등).

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.5	만 14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○협회 OO시스템은 만 14세 미만 아동도 이용이 가능하며, 회원가입 시 "만14세 이상 회원가입"과 "만14세 미만 회원가입"으로 가입 경로를 분리하여, 만14세 미만일 경우 법정대리인의 동의를 받아야 회원가입이 가능하도록 설계되어 있음				

회원가입 절차 (화면설계서)	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제22조(동의를 받는 방법) ⑥ 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.

【개인정보 보호법 시행령】

제17조(동의를 받는 방법) ④ 개인정보처리자는 법 제22조제6항에 따라 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있다.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제22조
- 개인정보 수집·제공 동의서 가이드라인(안)

세부분야	동의받는 방법의 적절성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.6	● **개인정보 관련 동의를 서면 등으로 받을 때에는 중요한 내용을 명확히 표시하여 알아보기 쉽게 하고, 개인정보 수집·이용, 제3자 제공, 목적 외 이용 등에 대해 각각 구분하여 동의를 받도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 정보주체의 동의에 의한 개인정보 수집 시 개인정보 수집·이용, 고유식별정보 처리, 민감정보 처리, 개인정보의 제3자 제공, 개인정보의 홍보·마케팅 이용 등의 일부만 각각의 동의를 받는 경우				
평가근거 및 의견	● ○○시스템에서 의료지원서비스를 위해 민감정보의 수집 및 ○○구청으로 ○○업무 수행을 위해 개인정보를 제공하고 있으나, 정보주체의 동의 시 제3자 제공에 대하여 구분하여 개별 동의를 받고, 민감정보는 구분하여 개별 동의를 받지 않음				

주요 점검 사항

1. 정보주체의 동의를 받을 때에는 개인정보의 수집 및 이용, 홍보 및 판매 권유를 위한 처리, 제3자 제공, 목적 외 이용 및 제공 등 각각의 동의사항을 구분하여 정보주체가 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.
2. 정정보주체에게 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는「개인정보 보호법 시행령」제17조제2항으로 정하는 내용을「개인정보 처리 방법에 관한 고시」제4조로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다..

① 개인정보보호법 시행령 제17조제2항으로 정하는 내용

- 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
- 「개인정보 보호법 시행령」제18조에 따른 민감정보, 시행령 제19조의 여권번호, 운전면허번호, 외국인등록번호
- 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
- 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

② 「개인정보 처리 방법에 관한 고시」제4조로 정하는 방법

- 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것
- 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
- 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

지표 해설

- 정보주체는 개인정보 처리에 대한 동의 여부를 결정하고 선택할 수 있는 권리가 보장되어 있으나, 실제로는 정보주체의 동의가 강제되는 경우가 많아 정보주체의 개인정보자기결정권을 보장하기 위하여 동의 방법을 법률로 구체화한 것이다.
- 개인정보처리자가 개인정보 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 받아야 하며, 정보주체가 동의를 구분해서 할 수 있다는 사실을 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 개인정보처리자는 목적에 필요한 최소한의 개인정보만을 수집하여야 하는바, 재화 또는 서비스 제공에 기본적으로 관련되는 사항과 부가적으로 관련되는 사항을 구분하여 이를 정보주체에게 알리고 동의를 받아야 한다.
- 정보주체의 개인정보보호를 위해서 실제로 정보주체가 동의한 사실이 명확히 확인될 수 있어야 하며, 개인정보처리자의 편의를 위해 일괄적으로 동의 여부를 묻는 전자우편을 발송한 후 거부 의사표시가 없을 경우 이를 동의로 간주하는 등의 방법은 적절하지 않다.
- 「개인정보 보호법」은 특히 정보주체가 좀 더 신중한 의사결정을 해야 할 필요가 있는 사항에 대해서는 동의의 내용과 의미를 명확하게 인지한 상태에서 동의 여부를 결정할 수 있도록 통상의 동의와 구분해서 별도의 동의를 받도록 하고 있다. 이때에도 개인정보처리자는 정보주체가 다른 개인정보처리의 목적과 별도로 동의 여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다.
- 다른 동의와 구분해서 별도 동의를 받아야 하는 경우에는 목적 외 이용·제공 동의(제18조제2항제1호), 개인정보를 제공받은 자의 이용·제공 제한(제19조제1호), 민감정보 처리 동의(제23조제1항제1호), 고유식별정보 처리 동의(제24조제1항제1호) 등이 해당된다. 예컨대, 고유식별정보를 수집할 때에는 「고유식별정보 수집·이용·제공에 대한 동의」를, 건강정보에 관한 정보를 수집할 때에는 「건강정보(민감정보) 수집·이용·제공에 대한 동의」를 별도로 분리해서 목적 등을 고지하고 동의를 받아야 한다.

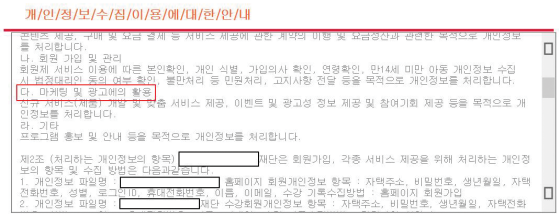
구분하여 동의를 받아야 하는 사항
● 개인정보 수집·이용 동의(법 제15조제1항제1호) ● 제3자 제공 동의(법 제17저제1항제1호) ● 국외 제3자 제공 동의(법 제17조제3항) ● 목적 외 이용·제공 동의(법 제18조제2항제1호) ● 마케팅 목적 처리 동의(법 제22조제4항) ● 법정대리인 동의(법 제22조제6항) ● 민감정보 처리 동의(법 제23조제1항제1호) ● 고유식별정보 처리 동의(법 제24조제1항제1호) 등

또한, 정보주체에게 동의를 받는 방법으로 「개인정보 보호법」 제22조제2항에 따라 동의를 서면(전자문서 포함)으로 받을 때에는 수집동의 안내 시 명확하게 표시하고 알아보기 쉽게 하여야 한다.

개인정보 수집·이용 동의시 고지 시 중요한 내용
1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보 주체에게 연락할 수 있다는 사실 2. 「개인정보 보호법 시행령」 제18조에 따른 민감정보, 시행령 제19조의 주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호 3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간) 4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

개인정보 수집·이용 동의시 고지 시 중요한 내용을 정하는 방법
1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것 2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것 3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.6	개인정보 관련 동의를 서면 등으로 받을 때에는 중요한 내용을 명확히 표시하여 알아보기 쉽게 하고, 개인정보 수집·이용, 제3자 제공, 목적 외 이용 등에 대해 각각 구분하여 동의를 받도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○기관은 홈페이지 회원가입 시 개인정보 수집이용에 대한 동의를 받고 있으며, 동의를 받는 방법 중 수집하는 개인정보를 마케팅 및 광고에의 활용 시에는 구분하여 별도의 동의를 받도록 하여야 하나, 개인정보 처리방침 내용의 일괄동의를 받고 있음. 회원가입 동의 안내  개/인/정/보/수/집/이/용/에/대/한/안/내 콘텐츠 제공, 구매 및 요금 결제 등 서비스 제공에 관한 계약의 이행 및 요금정산과 관련한 목적으로 개인정보를 처리합니다. 나. 회원 가입 및 관리 회원제 서비스 이용에 따른 본인확인, 개인 식별, 가입의사 확인, 연령확인, 만14세 미만 아동 개인정보 수집 시 법정대리인 동의 여부 확인, 불만처리 등 민원처리, 고지사항 전달 등을 목적으로 개인정보를 처리합니다. 다. 마케팅 및 광고에의 활용 신규 서비스(제품) 개발 및 맞춤 서비스 제공, 이벤트 및 광고성 정보 제공 및 참여기회 제공 등을 목적으로 개인정보를 처리합니다. 라. 기타 프로그램 홍보 및 안내 등을 목적으로 개인정보를 처리합니다. 제2조 (처리하는 개인정보의 항목) [redacted]재단은 회원가입, 각종 서비스 제공을 위해 처리하는 개인정보의 항목 및 수집 방법은 다음과같습니다. 1. 개인정보 파일명 : [redacted] 홈페이지 회원개인정보 항목 : 자택주소, 비밀번호, 생년월일, 자택전화번호, 성별, 로그인ID, 휴대전화번호, 이름, 이메일, 수강 기록수집방법 : 홈페이지 회원가입 2. 개인정보 파일명 : [redacted]재단 수강회원개인정보 항목 : 자택주소, 비밀번호, 생년월일, 자택전화 ☐ 이용약관에 동의합니다.				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 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.

③ 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.

④ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

【개인정보 보호법 시행령】

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 법 제22조제2항에서 "대통령령으로 정하는 중요한 내용"이란 다음 각 호의 사항을 말한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항
   가. 제18조에 따른 민감정보
   나. 제19조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호
3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

③ 개인정보처리자가 정보주체로부터 법 제18조제2항제1호 및 제22조제4항에 따른 동의를 받거나 법 제22조제3항에 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.

⑤ 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.

【개인정보 처리방법에 관한 고시】

제4조(서면 동의 시 중요한 내용 표시방법) 법 제22조제2항에서 "보호위원회가 고시로 정하는 방법"이란 다음 각 호의 방법을 말한다.

1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것
2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

【표준 개인정보 보호지침】

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.

⑤ 개인정보처리자는 법 제15조제1항제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제22조
- 개인정보 수집·제공 동의서 가이드라인(안)

세부분야	동의받는 방법의 적절성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.1.7	● **민감정보, 고유식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의를 받도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 정보주체의 동의에 의한 개인정보 수집 시 개인정보 수집·이용, 고유식별정보 처리 및 민감정보 처리에 대해 다른 개인정보 항목과 일괄로 동의를 받고 있는 경우				
평가근거 및 의견	● ○○시스템에서 의료지원서비스를 위해 의료법에 따라 의료행위를 위해 민감정보를 처리하고 있음. 다만, △△ 평가 업무에서 의료법에 따른 의료행위가 아닌 의료정보 제공 목적으로 사용하기 위해 민감정보를 수집하고 있으나, 정보주체의 동의 시 민감정보를 구분하여 별도 동의를 받지 않음				

주요 점검 사항

1. 민감정보의 처리는 원칙적으로 금지되어 있으므로, 민감정보의 수집 및 처리가 업무상 반드시 필요한지 검토되어야 한다.
2. 민감정보 또는 고유식별정보(주민등록번호 제외)의 수집·처리가 필요한 경우, 아래와 같이 정보주체의 별도 동의를 받거나 법령에 근거해야 한다.
   ① 다른 개인정보의 처리에 대한 동의와 **별도로** 동의를 받는 경우
   ② 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
   ③ 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

지표 해설

- 본 지표에서는 개인정보 흐름분석 결과를 바탕으로 평가대상 업무 중에 민감정보, 고유식별정보의 처리가 존재하는 경우 별도 동의 등 적법하게 수집하는 지 여부에 대해 평가한다.
- 민감정보는 원칙적으로 처리가 금지되어 있으며, 정보주체의 명시적 동의가 있거나 법령에 근거가 있는 등 예외적인 사유가 있을 때에만 처리를 인정하고 있다. 결국 정보주체의 별도 동의를 받는 경우에는 민감정보의 수집·처리가 가능하지만 법의 취지를 고려할 때 업무상 반드시 필요한 것이 아니라면 수집 및 처리를 하지 않는 것이 바람직하다.

민감정보의 유형
1. 사상 · 신념 (이데올로기, 사상적 경향, 종교적 신념 등) 2. 노동조합 · 정당의 가입 · 탈퇴 (반드시 적법한 노동조합이거나 정당일 필요는 없음) 3. 정치적 견해 (정치적 사안에 대한 입장, 특정 정당의지지 여부에 관한 정보 등) 4. 건강, 성생활 등에 관한 정보 (병력(病歷), 신체적·정신적 장애, 성적취향 등, 혈액형은 제외) 5. 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보 - 유전자검사 등의 결과로 얻어진 유전정보 - 형의 선고·면제 및 선고 유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소 등 범죄경력에 관한 정보 - 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보 - 인종이나 민족에 관한 정보

- 「개인정보 보호법 시행령」에 따른 민감정보(유전정보, 범죄경력에 관한 정보)는 공공기관이 다음의 업무수행을 위하여 처리하는 경우에는 민감정보로 보지 않는다.
  - 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보보호위원회의 심의·의결을 거친 경우
  - 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
  - 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
  - 법원의 재판업무 수행을 위하여 필요한 경우
  - 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

- 고유식별정보란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호가 이에 해당된다.

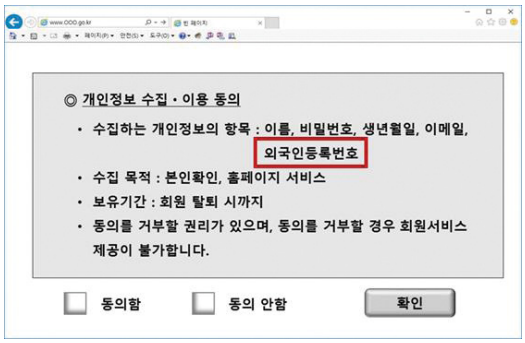
고유식별정보의 유형
1. 「주민등록법」 제7조제3항에 따른 주민등록번호 2. 「여권법」 제7조제1항제1호에 따른 여권번호 3. 「도로교통법」 제80조에 따른 운전면허의 면허번호 4. 「출입국관리법」 제31조제4항에 따른 외국인등록번호

- 고유식별정보도 민감정보와 마찬가지로 원칙적으로 처리할 수 없다. 다만 별도로 정보주체의 동의를 받는 경우와 법령에서 고유식별정보의 처리를 요구하거나 허용하고 있는 경우에는 예외가 인정된다. 하지만 주민등록번호에 한해서는 '주민등록번호 수집 법정주의'에 따라 법률, 시행령 등에 근거가 없다면 정보주체의 별도 동의를 받는다 하더라도 주민등록번호의 수립 및 처리는 금지된다.

- 정보주체의 별도 동의를 받는 경우에는 「개인정보 보호법」 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보 처리에 대한 동의와 분리해서 동의를 받아야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.1.7	민감정보, 고유식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의를 받도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○기관은 홈페이지 회원가입 시 외국인에 대하여 외국인등록번호(고유식별정보)를 수집하고 있으나 이름, 생년월일 등 다른 개인정보 항목과 함께 일괄로 동의를 받도록 설계되어 있음				

회원가입 동의 안내 (화면설계서)	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 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.

제23조(민감정보의 처리 제한) ① 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

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.

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

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.

【개인정보 보호법 시행령】

제18조(민감정보의 범위) 법 제23조제1항 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
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 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

제62조의2(민감정보 및 고유식별정보의 처리) ① 보호위원회(제62조제3항에 따라 보호위원회의 권한을 위탁받은 자를 포함한다)는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 법 제23조에 따른 민감정보와 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제7조의9제1항제4호부터 제6호까지의 규정에 따른 사항의 심의 · 의결에 관한 사무
2. 법 제24조의2제4항에 따른 주민등록번호 대체 방법 제공을 위한 시스템 구축 등 제반조치 마련 및 지원에 관한 사무
3. 법 제28조의6, 제34조의2 및 제39조의15에 따른 과징금의 부과 및 징수에 관한 사무
4. 법 제62조제3항에 따른 개인정보침해 신고센터의 업무에 관한 사무
5. 법 제63조제1항, 제2항 및 제7항에 따른 자료의 제출, 검사 및 점검에 관한 사무

② 분쟁조정위원회는 법 제45조 및 제47조에 따른 개인정보 분쟁 조정에 관한 사무를 수행하기 위하여 불가피한 경우 법 제23조에 따른 민감정보와 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제23조, 제24조

2 보유

세부분야	보유기간 산정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.2.1	● **개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소 기간을 초과한 기간으로 산정하여 보유하고 있는 경우				
평가근거 및 의견	● ○○○공사는 인터넷 쇼핑몰을 운영하면서 '소비자의 불만 또는 분쟁처리에 관한 기록'을 「전자상거래 등에서의 소비자보호에 관한 법」 시행령 제3조제1항제4호에 명시된 보유기간인 3년을 초과하여 5년간 보관하고 있음				

주요 점검 사항

1. 개인정보의 보유기간은 관련 법령기준 및 보유목적에 부합된 최소 기간으로 산정하여야 한다.
2. 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의 및 내부 결재 등 공식적인 절차를 통해 산정하여야 한다.

지표 해설

- 본 지표에서는 평가대상이 되는 개인정보파일 별로 보유기간이 필요 최소한의 기간으로 산정되었는지 여부를 평가한다.
- 개인정보를 보유하려는 경우에는 관련 법적 기준 및 보유 목적에 부합된 최소의 기간으로 보유기간을 산정하여야 한다.
  - 법령에 보유기간이 명시된 경우 : 해당 법령 기준으로 보유기간 산정
  - 법령에 보유목적이 명시된 경우 : 해당 법령에 명시된 보유목적 달성 시까지
  - 정보주체의 동의를 받고 수집하는 경우 : 해당 수집 목적 달성 시까지
- 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 및 내부 결재를 통하여 보유기간을 산정하여야 한다. 공공기관의 경우 「표준 개인정보 보호지침」 별표1의 '개인정보파일 보유기간 책정 기준표' 및 「공공기록물 관리에 관한 법률 시행령」에 따른 기록관리기준표를 상회할 수 없다.

개인정보파일 보유기간 책정 기준표(표준 개인정보 보호지침 별표1)	
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

기록물의 보존기간별 책정기준(「공공기록물 관리에 관한 법률」 시행령 별표1)	
보유기간	대상기록물
영구	1. 공공기관의 핵심적인 업무수행을 증명하거나 설명하는 기록물 중 영구 보존이 필요한 기록물 2. 국민이나 기관 및 단체, 조직의 지위, 신분, 재산, 권리, 의무를 증명하는 기록물 중 영구보존이 필요한 기록물 3. 국가나 지역사회의 역사경험을 증명할 수 있는 기록물 중 영구보존이 필요한 기록물 4. 국민의 건강증진, 환경보호를 위하여 필요한 기록물 중 영구보존이 필요한 기록물 5. 국민이나 기관 및 단체, 조직에 중대한 영향을 미치는 주요한 정책, 제도의 결정이나 변경과 관련된 기록물 중 영구보존이 필요한 기록물 6. 인문·사회·자연 과학의 중요한 연구성과와 문화예술분야의 성과물로 국민이나 기관 및 단체, 조직에 중대한 영향을 미치는 사항 중 영구보존이 필요한 기록물 7. 공공기관의 조직구조 및 기능의 변화, 권한 및 책무의 변화, 기관장 등 주요직위자의 임면 등과 관련된 기록물 중 영구보존이 필요한 기록물 8. 일정 규모 이상의 국토의 형질이나 자연환경에 영향을 미치는 사업·공사 등과 관련된 기록물 중 영구보존이 필요한 기록물

기록물의 보존기간별 책정기준(「공공기록물 관리에 관한 법률」 시행령 별표1)	
보유기간	대상기록물
	9. 제17조제1항 각 호의 어느 하나에 해당하는 사항에 관한 기록물 중 영구보존이 필요한 기록물 10. 제18조제1항 각 호의 어느 하나에 해당하는 회의록 중 영구보존이 필요한 기록물 11. 제19조제1항 각 호의 어느 하나에 해당하는 시청각기록물 중 영구보존이 필요한 기록물 12. 국회 또는 국무회의의 심의를 거치는 사항에 관한 기록물중 영구보존이 필요한 기록물 13. 공공기관의 연도별 업무계획과 이에 대한 추진과정, 결과 및 심사분석 관련 기록물, 외부기관의 기관에 대한 평가에 관한 기록물 14. 대통령, 국무총리의 지시사항과 관련된 기록물중 영구보존이 필요한 기록물 15. 백서, 그 밖에 공공기관의 연혁과 변천사를 규명하는데 유용한 중요 기록물 16. 다수 국민의 관심사항이 되는 주요 사건 또는 사고 및 재해관련 기록물 17. 대통령, 국무총리 관련 기록물과 외국의 원수 및 수상 등의 한국 관련 기록물 18. 토지 등과 같이 장기간 존속되는 물건 또는 재산의 관리, 확인, 증명에 필요한 중요 기록물 19. 장·차관급 중앙행정기관 및 광역자치단체의 장의 공식적인 연설문, 기고문, 인터뷰 자료 및 해당 기관의 공식적인 브리핑 자료 20. 국회와 중앙행정기관 간, 지방의회와 지방자치단체 간 주고받은 공식적인 기록물 21. 외국의 정부기관 혹은 국제기구와의 교류협력, 협상, 교류활동에 관한 주요 기록물 22. 공공기관 소관 업무분야의 통계·결산·전망 등 대외발표 혹은 대외 보고를 위하여 작성한 기록물 23. 영구기록물관리기관의 장 및 제3조 각 호의 어느 하나에 해당하는 공공기관의 장이 정하는 사항에 관한 기록물 24. 다른 법령에 따라 영구 보존하도록 규정된 기록물 24의2. 기관의 조직, 기능 및 기관과 국민 간의 의사소통 등에 관한 웹기록물 및 웹기록물 관련 시스템의 구축 · 운영과 관련된 중요한 기록물 25. 그 밖에 역사자료로서의 보존가치가 높다고 인정되는 기록물
준영구	1. 국민이나 기관 및 단체, 조직의 신분, 재산, 권리, 의무를 증빙하는 기록물 중 관리대상 자체가 사망, 폐지, 그 밖의 사유로 소멸되기 때문에 영구보존할 필요성이 없는 기록물 2. 비치기록물로서 30년 이상 장기보존이 필요하나, 일정기간이 경과하면 관리대상 자체가 사망, 폐지, 그 밖의 사유로 소멸되기 때문에 영구보존의 필요성이 없는 기록물 3. 국민이나 기관 및 단체, 조직의 권리, 신분 증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터셋(dataset) 및 운영시스템의 구축과 관련된 중요한 기록물 4. 토지수용, 「보안업무규정」 제30조에 따른 보호구역 등 국민의 재산권과 관련된 기록물 중 30년 이상 보존할 필요가 있는 기록물 5. 관계 법령에 따라 30년 이상의 기간 동안 민·형사상 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 사항에 관한 기록물 6. 그 밖에 역사자료로서의 가치는 낮으나 30년 이상 장기보존이 필요하다고 인정되는 기록물
30년	1. 영구·준영구적으로 보존할 필요는 없으나 공공기관의 설치목적을 구현하기 위한 주요업무와 관련된 기록물로서 10년 이상의 기간 동안 업무에 참고하거나 기관의 업무 수행 내용을 증명할 필요가 있는 기록물 2. 장·차관, 광역자치단체장 등 고위직 기관장의 결재를 필요로 하는 일반적인 사항에 관한 기록물 3. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 사항에 관한 기록물

기록물의 보존기간별 책정기준(「공공기록물 관리에 관한 법률」 시행령 별표1)	
보유기간	대상기록물
	4. 다른 법령에 따라 10년 이상 30년 미만의 기간 동안 보존하도록 규정한 기록물 5. 그 밖에 10년 이상의 기간 동안 보존할 필요가 있다고 인정되는 기록물
10년	1. 30년 이상 장기간 보존할 필요는 없으나 공공기관의 주요업무에 관한 기록물로 5년 이상의 기간동안 업무에 참고하거나 기관의 업무 수행 내용을 증명할 필요가 있는 기록물 2. 본부·국·실급 부서장의 전결사항으로 공공기관의 주요업무를 제외한 일반적인 사항과 관련된 기록물 3. 관계 법령에 따라 5년 이상 10년 미만의 기간동안 민·형사상 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 사항에 관한 기록물 4. 다른 법령에 따라 5년 이상 10년 미만의 기간 동안 보존하도록 규정한 기록물 5. 그 밖에 5년 이상 10년 미만의 기간 동안 보존할 필요가 있다고 인정되는 기록물
5년	1. 처리과 수준의 주요한 업무와 관련된 기록물로서 3년 이상 5년 미만의 기간 동안 업무에 참고하거나 기관의 업무 수행 내용을 증명할 필요가 있는 기록물 2. 기관을 유지하는 일반적인 사항에 관한 예산·회계 관련 기록물(10년 이상 보존대상에 해당하는 주요 사업 관련 단위과제에 포함되는 예산·회계 관련 기록물의 보존기간은 해당 단위과제의 보존기간을 따른다) 3. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민사상·형사상 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 사항에 관한 기록물 4. 다른 법령에 따라 3년 이상 5년 미만의 기간 동안 보존하도록 규정한 기록물 5. 그 밖에 3년 이상 5년 미만의 기간 동안 보존할 필요가 있다고 인정되는 기록물
3년	1. 처리과 수준의 일상적인 업무를 수행하면서 생산한 기록물로서 1년 이상 3년 미만의 기간 동안 업무에 참고하거나 기관의 업무 수행 내용을 증명할 필요가 있는 기록물 2. 행정업무의 참고 또는 사실의 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 기록물 3. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민·형사상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 사항에 관한 기록물 4. 다른 법령에 따라 1년 이상 3년 미만의 기간 동안 보존하도록 규정한 기록물 5. 그 밖에 1년 이상 3년 미만의 기간 동안 보존할 필요가 있다고 인정되는 기록물 6. 각종 증명서 발급과 관련된 기록물(다만, 다른 법령에 증명서 발급 관련 기록물의 보존기간이 별도로 규정된 경우에는 해당 법령에 따름) 7. 처리과 수준의 주간·월간·분기별 업무계획 수립과 관련된 기록물
1년	1. 행정적·법적·재정적으로 증명할 가치가 없으며, 역사적으로 보존하여야할 필요가 없는 단순하고 일상적인 업무를 수행하면서 생산한 기록물 2. 기관 내 처리과간에 접수한 일상적인 업무와 관련된 사항을 전파하기 위한 지시공문 3. 행정기관 간의 단순한 자료요구, 업무연락, 통보, 조회 등과 관련된 기록물 4. 상급기관(부서)의 요구에 따라 처리과의 현황, 업무수행 내용 등을 단순히 보고한 기록물(취합부서에서는 해당 단위과제의 보존기간 동안 보존하여야 한다)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.2.1	개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정하도록 계획하고 있습니까?		○		

평가근거 및 의견

● ○○○기관은 영향평가 수행 중 확인된 3개의 개인정보파일 중 2개는 최소한의 보유기간으로 산정되어 있으나, '개인정보보호 전문강사' 개인정보파일의 경우에는 실제 전문강사 활동기간인 3년을 초과하여 5년간 해당 개인정보파일을 보유하는 것으로 되어 있음

개인정보파일명	평가업무	분석내용
○○파일	AA업무	법률에 따라 3년간 보관하고 있음
○○파일	BB업무, CC업무	보유기간 3년으로 적정함
○○파일	전문강사관리	보유기간 5년으로 보관하고 있음 (3년으로 변경 필요)

개인정보 파일 등록 내역

관련법령 및 문서

관련 법령 · 지침

【공공기록물 관리에 관한 법률 시행령】

제26조(보존기간) ① 기록물의 보존기간은 영구, 준영구, 30년, 10년, 5년, 3년, 1년으로 구분하며, 보존기간별 책정 기준은 별표 1과 같다. 다만, 「대통령기록물 관리에 관한 법률」 제2조제1호에 따른 대통령기록물, 수사·재판·정보·보안 관련 기록물은 소관 중앙행정기관의 장이 중앙기록물관리기관의 장과 협의하여 보존기간의 구분 및 그 책정 기준을 달리 정할 수 있다.

②기록물의 보존기간은 단위과제별로 책정한다. 다만, 영구기록물관리기관의 장은 특별히 보존기간을 달리 정할 필요가 있다고 인정되는 단위과제에 대하여는 보존기간을 직접 정할 수 있다.

③보존기간의 기산일은 단위과제별로 기록물의 처리가 완결된 날이 속하는 다음 연도의 1월 1일로 한다. 다만, 여러 해에 걸쳐서 진행되는 단위과제의 경우에는 해당 과제가 종결된 날이 속하는 다음 연도의 1월 1일부터 보존기간을 기산한다.

【표준 개인정보 보호지침】

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.

3 이용·제공

세부분야	개인정보 제공의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.1	● **개인정보를 제3자에게 제공하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 정보주체의 별도 동의를 받거나 관련 법률에 근거하여 제3자 제공을 하고 있으나, 제공하는 개인정보 항목, 보유기간 등 그 사항이 동의받은 내용 및 법률내용과 불일치 하는 경우				
평가근거 및 의견	● ○○협회의 평가업무 중 AA평가업무는 ○○법에 의거하여 ○○업무수행 목적으로 A기관으로 개인정보를 제공하고 있으나, BB평가업무는 B기관에 제공하는 것에 대한 법적 근거가 없어 제3자 제공 동의를 받아야 하나 동의를 받고 있지 않음				

주요 점검 사항

1. 개인정보를 제3자에게 제공하는 경우에는 아래와 같이 적법한 근거가 있어야 한다.
   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 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
2. 정보주체의 동의를 받는 경우에는 관련 사항을 모두 알려야 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. 개인정보를 국외의 제3자에게 제공할 때에는 정보주체의 동의를 받아야 하며, 개인정보 보호법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하지 않아야 한다.
4. 정보주체의 동의 여부, 동의 일시 등을 사후에 확인할 수 있도록 개인정보처리시스템에 관련 내용이 기록되어야 한다.

※ 개인정보 흐름분석 결과를 바탕으로 모든 평가업무에 대해 제공 흐름별로 빠짐없이 점검 필요

지표 해설

● 개인정보의 제3자 제공이란 개인정보처리자 외의 제3자에게 개인정보의 지배·관리권이 이전되는 것을 의미한다. 즉 개인정보를 저장한 매체나 수기문서를 전달하는 경우뿐만 아니라 DB 시스템에 대한 접속권한을 허용하여 열람·복사가 가능하게 하여 개인정보를 공유하는 경우 등도 '제공'에 포함된다. 한편, 민감정보 및 고유식별정보를 제3자에게 제공하는 경우에는 제23조, 제24조 및 제24조의2를 따라야 한다.

목적 외 이용, 영업양도 등과의 차이		
목적외 이용과의 차이	처리업무 위탁과의 차이	영업양도 등과의 차이
개인정보의 제3자 제공이란 개인정보처리자 외의 제3자에게 개인정보의 지배·관리권이 이전되는 것을 말한다. 반면 목적외 이용이란 같은 개인정보처리자(기관, 단체, 법인 등) 내에서 당초의 수집목적을 벗어나서 개인정보를 이용하는 것을 말한다. 같은 개인정보처리자 내에서 당초 수집목적과 다른 목적에 이용하기 위해 서로 다른 부서 간에 개인정보를 제공하는 것은 제3자 제공이 아니라 목적 외 이용에 해당된다.	업무위탁과 개인정보 제3자 제공 모두 개인정보가 다른 사람(제3자)에게 이전되거나 공동으로 이용하게 된다는 측면에서는 동일하다. 그러나 '업무위탁'의 경우에는 개인정보처리자의 업무를 처리할 목적으로 개인정보가 제3자(수탁자)에게 이전되지만, '제3자 제공'은 그 제3자의 업무를 처리할 목적 및 그 제3자의 이익을 위해서 개인정보가 이전된다는 점이 다르다. 또한 업무위탁의 경우에는 개인정보처리자의 관리·감독을 받지만, 제3자 제공은 개인정보가 제공된 이후에는 제3자가 자신의 책임 하에 개인정보를 처리하게 되며, 개인정보처리자의 관리·감독권이 미치지 못한다.	영업의 양도·합병(제27조)는 비록 개인정보가 제3자에게 이전된다는 점에서는 '제3자 제공'과 유사하다. 그러나 영업의 양도·합병은 그 개인정보를 이용한 업무의 형태는 변하지 않고 단지 개인정보의 관리주체만 변한다는 점에서 '제3자 제공'과는 차이가 있다. 이에 따라 영업의 양도·합병에 대해서는 이 법 제27조에서 별도의 규정을 두고 있으며, 제3자 제공과 관련한 규정은 적용되지 않는다.

● 개인정보를 제3자에게 제공할 때에는 다음의 경우에 해당되어야 한다.(①~④)

① 정보주체의 동의를 받는 경우

개인정보처리자가 제3자 제공에 대한 동의를 받을 때에는 정보주체게 제3자 제공의 내용과 의미를 명확히 알 수 있도록 미리 개인정보를 제공받는 자의 성명 등을 미리 알려주어야 하며, 알려야 할 사항 중 어느 하나에 변경이 있는 경우에도 정보주체에게 변경 사실을 알리고 다시 동의를 받아야 한다.

개인정보 제3자 제공 동의 시 고지 사항
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 동의거부에 따른 불이익이 있는 경우 그 불이익의 내용 ※ '개인정보를 제공받는 자'란 제공받는 자의 이름 또는 상호를 의미하므로, 금융기관, 정부기관 등과 같이 정보주체가 제공받는 자를 알기 어렵도록 포괄적으로 알리는 것은 안 됨. 또한 제공받는 자가 여러 명일 경우에는 각각의 이름 또는 상호를 알리고 제공되는 목적, 항목, 기간 등이 다를 경우에는 제공받는 자별로 그 목적, 항목, 기간 등을 각각 알려야 함

개인정보 제3자 제공 동의 양식 예시

제공 받는 자	제공 항목	제공 목적	보유 기간
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 ○○○ 서비스의 이용에 제한을 받을 수 있습니다.

위와 같이 개인정보를 제공하는데 동의하십니까?	□ 동의함	□ 동의하지 않음

② 법률규정이 있거나 법령상 의무준수를 위해 불가피한 경우

- **법률의 특별한 규정** : 법률에서 개인정보의 수집·이용을 구체적으로 요구하거나 허용하고 있어야 한다. 수집·이용할 수 있는 개인정보의 대상·범위가 막연한 경우는 특별한 규정이라고 할 수 없다. 법률에 특별한 규정이 있어야 하므로 시행령이나 시행규칙에 규정하는 것은 안 된다. 시·군·구의 장의 공직선거 입후보자에 대한 선거인명부 교부(「공직선거법」 제46조), 보험요율산출기관의 보험회사에 대한 보험계약자 교통법규위반 개인정보 제공(「보험업법」 제176조), 교통사고환자를 치료한 의료기관의 보험회사 등에 대한 진료기록 열람허용(「자동차손해배상보장법」 제14조) 등의 의무를 준수하기 위하여 개인정보처리자는 정보주체의 동의 없이 개인정보를 관계 당사자에게 제공할 수 있다.

- **법령상 의무준수** : 법령에서 개인정보처리자에게 일정한 의무를 부과하고 있는 경우로서 해당 개인정보처리자가 그 의무 이행을 위해서 개인정보를 불가피하게 수집·이용할 수밖에 없는 경우를 말한다. 법률에 의한 의무뿐만 아니라 시행령, 시행규칙에 따른 의무도 포함된다. '불가피한 경우'란 개인정보를 수집하지 않고는 법령에서 부과하는 의무를 이행하는 것이 불가능하거나 개인정보처리자가 다른 방법을 사용하여 의무를 이행하는 것이 현저히 곤란한 경우를 의미한다. 의료인·의료기관의 보건당국에 대한 감염병 환자 신고의무(「감염병의 예방 및 관리에 관한 법률」 제11조), 외국환을 거래하는 금융당국의 해외 송금자 국세청 통보의무(「외국환거래법」 제21조), 소득지급자의 소득귀속자에 대한 원천징수의무 및 원천징수이행상황신고의무(「소득세법」 제127조 및 제128조) 등을 이행하기 위한 개인정보의 제공이 법령상 의무 준수의 예에 속한다.

③ 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우

공공기관의 경우에는 법령 등에서 정해진 소관업무를 수행하기 위하여 수시로 개인정보를 제3자에게 제공해야 할 필요가 있다. 공공기관의 경우에는 개인정보를 수집할 수 있도록 명시적으로 허용하는 법률 규정이 없더라도 법령 등에서 소관업무를 정하고 있고 그 소관 업무의 수행을 위하여 불가피하게 개인정보를 수집할 수밖에 없는 경우에는 정보주체의 동의 없이 개인정보의 수집이 허용된다.

'법령 등에서 정하는 소관업무'란 「정부조직법」 및 각 기관별 직제·직제규칙, 개별 조직법 등에서 정하고 있는 소관사무 이외에, 「주민등록법」, 「국세기본법」, 「의료법」, 「국민건강보험법」 등 소관법령에 의해서 부여된 권한과 의무,

지방자치단체의 경우 조례에서 정하고 있는 업무 등을 의미한다. 지방자치단체의 경우 다양한 인허가사무, 신고수리, 복지업무, 관리·감독 등의 업무를 수행해야 하기 때문에 실무적으로 개인정보를 제3자에게 제공해야 하는 경우가 자주 발생할 수 있다.

공공기관이 소관 업무를 수행하기 위하여 개인정보를 제3자에게 제공함에 있어서는 정말로 불가피한 사유가 있는지 여부를 신중하게 검토해야 한다. '불가피한 경우'란 개인정보를 제공하지 아니하고는 법령 등에서 해당 공공기관에 부여하고 있는 권한의 행사나 의무의 이행이 불가능 하거나 다른 방법을 사용하여 소관 업무를 수행하는 것이 현저히 곤란한 경우를 의미한다. 특히 공공기관이 내부고발, 민원업무 등을 처리하기 위하여 민원인의 개인정보를 제3자에게 제공할 때에는 주의해야 한다. 민원업무를 쉽게 해결하기 위하여 민원인의 개인정보를 피민원이나 피민원 기관에 제공하는 것은 불가피한 필요가 있는 경우라고 보기 어렵다.

④ 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 제3자의 급박한 생명·신체·재산상의 이익을 위하여 필요하다고 인정되어 개인정보를 수집하였다면 그 수집 목적 범위에서 정보주체의 동의 없이 개인정보를 제3자에게 제공할 수 있다. 동사무소나 경찰관서가 시급히 수술 등의 의료조치가 필요한 교통사고 환자의 연락처를 의료기관에 알려주는 행위가 이에 속한다.

- 개인정보의 국외 제3자 제공은 개인정보처리자가 개인정보를 국외의 제3자에게 '제공'하고자 할 때에는 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처, ② 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의 거부권이 존재하다는 사실 및 동의 거부에 따른 불이익이의 내용(불이익이 있는 경우에 한함)을 모두 정보주체에게 알리고 동의를 받아야 한다(제3항 전단). 국내외를 불문하고 개인정보를 제3자에게 제공할 때에는 동의획득의무와 고지의무가 부과되어 있다.
- 개인정보 제3자 제공 동의를 받은 사항에 대해서는 사후 분쟁발생 시 증빙자료 제출 및 정보주체의 개인정보 열람 요구 등에 대응하기 위해서 기록을 남겨야 한다. 해당 기록에는 제공받는 자, 제공 목적, 제공 일시, 동의 여부 및 동의 일시 등 관련 사항을 모두 포함하여야 한다.
- 개인정보 국외 이전은 국외 제공보다 개념이 넓다. 국외의 제3자에게 개인정보를 제공하는 것은 물론이고, 개인정보처리를 국외의 제3자에게 위탁하기 위해 국외로 옮겨지는 경우도 국외 이전에 포함된다. 위탁의 경우 정보주체의 동의를 받을 필요는 없지만 처리위탁에 관한 규정(제26조)에 따라야 한다.

유형별 국외이전 사례
● 제3자 제공형 : 해외 여행업을 하는 사업자가 외국 협력사에게 고객정보를 제공하는 경우, 다국적기업의 한국 지사가 수집한 고객정보를 미국 본사로 이전하는 경우 ● 해외 위탁형 : 인건비가 저렴한 중국에 자회사를 설치하고 국내 고객DB를 이용해 콜센터업무(고객대응업무)를 대행시키는 경우 ● 직접 수집형 : 해외 인터넷쇼핑몰 사업자가 국내 소비자의 개인정보를 해외에서 직접 수집하는 경우

평가 예시

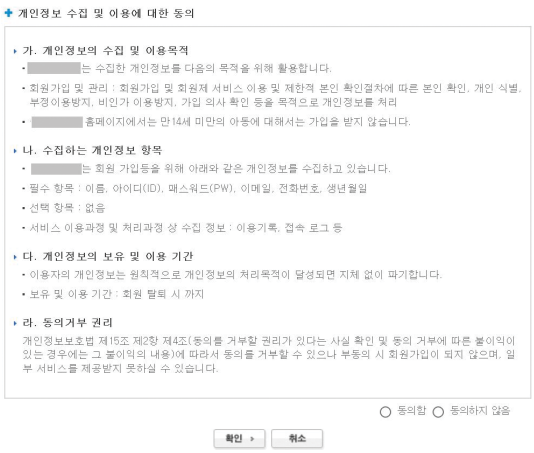
구 분	질의문	이행	부분이행	미이행	해당없음
3.3.1	개인정보를 제3자에게 제공하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?		○		

평가근거 및 의견

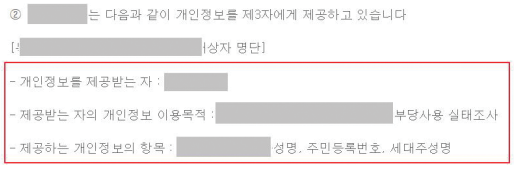
- ○○관은 대상시스템의 10개 평가업무 중 3개의 평가업무가 개인정보 흐름표에서 제공을 하고 있음
- AA업무, BB업무는 법령의 의무준수를 위해 불가피한 경우로 제공하고 있음
- 하지만, CC업무의 경우 별도의 법적 근거가 없어 정보주체의 제3자 제공 동의가 필요하나 화면설계 등 설계문서에 정보주체의 제3자 제공 동의절차가 설계되어 있지 않음.

평가업무명	제공근거	분석내용
AA업무	OO법률 제0조	법률에 규정하고 있음
BB업무	OO법률 시행령 제0조	법령상 의무준수를 위해 불가피한 경우
CC업무	정보주체의 동의	정보추체 제3자 제공 동의 누락됨

개인정보 수집 및 이용에 대한 동의양식



개인정보 처리방침 (제3자 제공사항)



관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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 · 제5호 및 제39조의3제2항제2호 · 제3호에 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.

④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

【표준 개인정보 보호지침】

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.

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제17조
- 개인정보 수집·제공 동의서 가이드라인(안)

세부분야	개인정보 제공의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.2	● **개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보를 목적 외 제3자 제공 시 최소한의 항목으로 제한하지 않은 경우				
평가근거 및 의견	● ○○기관 복지시스템에서 포인트 결제와 관련하여 구매자의 결제정보를 카드사에 제공하고 있으나, 제공 시 결제정보 이외의 회사정보(회사명, 회사주소, 직책, 연봉) 등을 추가로 제공하고 있음				

주요 점검 사항

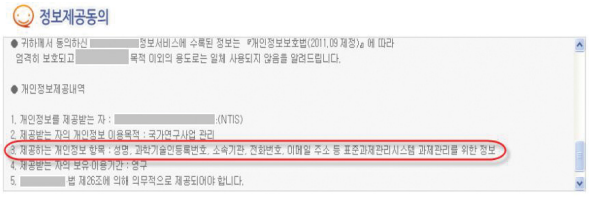
1. 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 항목만 제공되어야 한다.

지표 해설

- 3.3.1【지표 해설】 참조
- 다른 기관에 개인정보를 제공할 경우에는 제공에 필요한 개인정보 항목을 정의하고 타당성을 검토한 후 업무 수행에 필요한 최소한의 항목만을 제공해야 한다.
- 법률 규정, 법령상 의무 준수 및 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 필요한 경우에는 정보주체의 동의 없이 제3자 제공이 가능하도록 규정되어 있으나, 이때에도 "불가피한 경우"로 한정하고 있다. 결국 법령 등에 따라 개인정보를 제3자에게 제공하는 경우에는 업무 수행에 필요한 "최소한의 개인정보"만을 제공하여야 한다.
- 정보주체의 동의를 받고 제3자에게 제공하는 경우라 할지라도, 최소 수집의 원칙에 따라 해당 제공목적에 필요한 최소한의 개인정보로 한정하는 것이 바람직하다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.3.2	개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?			○	
평가근거 및 의견	● A기관은 ○○법에 의거 수집하는 개인정보에 대하여 ○○기관으로 제3자 제공을 하며, 제공내용을 정보주체로부터 안내하고 동의를 받고 있으나 제공하는 항목에 대하여 ○○법 제26조에는 성명, 소속기관, 과학기술인증등록번호, ○○○시스템 관리를 위한 정보 등이 명시되어 있고, A기관에서 ○○기관으로 제공하는 항목에는 이메일, 전화번호 등 일부 법에 명시된 항목을 초과하여 제공하고 있음.				

정보제공 동의	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

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 · 제5호 및 제39조의3제2항제2호 · 제3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

관련 문서

● 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제17조

세부분야	목적 외 이용 · 제공 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.3	● **개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 별도의 동의를 받거나 관련 법률에 근거하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 평가업무 일부에서 정보주체의 별도 동의를 획득하거나 관련 법률 근거없이 개인정보를 목적 외의 용도로 이용하는 경우				
평가근거 및 의견	● ○○대학교는 AA업무에 대하여 병역법에 근거하여 제공하고 있으나, BB업무에서 졸업생정보를 △△기관 제공하는 것은 별도의 법률에 규정되어 있지 않으므로 별도의 동의를 받아야 하지만 별도 동의를 받고 있지 않음				

주요 점검 사항

1. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 경우, 아래와 같이 별도의 동의를 받거나 법률 등에 근거하여야 한다.
   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 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 소관업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
   ⑥ 조약, 그 밖의 국제 협정의 이행을 위하여 외국정보 또는 국제기구에 제공하기 위하여 필요한 경우
   ⑦ 범죄의 수바와 공소의 제기 및 유지를 위하여 필요한 경우
   ⑧ 법원의 재판업무 수행을 위하여 필요한 경우
   ⑨ 형(形)의 감호, 보호처분의 집행을 위하여 필요한 경우

2. 개인정보의 목적 외 이용 또는 제공에 따른 동의를 받는 경우에는 아래와 같이 필요한 사항을 모두 알려야 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 이용기간을 말한다)
   ⑤ 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

3. 개인정보를 통계작성 및 학술연구 등의 목적을 위하여 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우, 재식별화의 위험을 최소화할 수 있도록 적정한 방법을 선정하여 비식별화 조치를 적용하여야 한다.
   ※ 개인정보 흐름분석 결과를 바탕으로 모든 목적 외 이용 및 제3자 제공 흐름에 대해 빠짐없이 점검 필요

지표 해설

- 개인정보처리자는 정보주체에게 이용·제공의 목적을 고지하고 동의를 받거나 이 법 또는 다른 법령에 의하여 이용·제공이 허용된 범위를 벗어나서 개인정보를 이용하거나 제공해서는 안 된다.

목적 외 이용 사례
● 공무원들에게 업무용으로 발급한 이메일 계정 주소로 사전 동의절차 없이 교육 등 마케팅 홍보자료를 발송한 경우 ● 조세 담당 공무원이 자신과 채권채무 관계로 소송 중인 사람에 관한 납세정보를 조회하여 소송에 이용한 경우 ● 상품배송을 목적으로 수집한 개인정보를 사전에 동의받지 않은 자사의 별도 상품·서비스의 홍보에 이용 ● 고객 만족도 조사, 판촉행사, 경품행사에 응모하기 위하여 입력한 개인정보를 사전에 동의받지 않고 자사의 할인판매 행사 안내용 광고물 발송에 이용 ● A/S센터에서 고객 불만 및 불편 사항을 처리하기 위해 수집한 개인정보를 자사의 신상품 광고에 이용 ● 공개된 개인정보의 성격과 공개 취지 등에 비추어 그 공개된 목적을 넘어 DB마케팅을 위하여 수집한 후 이용하는 행위

목적 외 제공 사례
● 주민센터 복지카드 담당 공무원이 복지카드 신청자의 개인정보(홍보 마케팅 등으로 개인정보 제공을 동의하지 않은 경우)를 정보주체의 동의 없이 사설학습지 회사에 제공 ● 홈쇼핑 회사가 주문상품을 배달하기 위해 수집한 고객정보를 정보주체의 동의 없이 계열 콘도미니엄사에 제공하여 콘도미니엄 판매용 홍보자료 발송에 활용

- 「개인정보 보호법」 제18조제2항제1호부터 제9호는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있는 예외적인 사유를 규정하고 있다. 다만 이 경우에도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때에는 개인정보를 목적외의 용도로 이용하거나 제3자에게 제공할 수 없으며, 제5호부터 제9호까지의 사유는 공공기관이 처리하는 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우에 한정한다.

① 정보주체로부터 별도의 동의를 받는 경우

개인정보를 수집 목적을 넘어 이용하거나, 제공하는 경우 다른 개인정보의 처리에 대한 동의와 분리해서 목적외 이용·제공에 대한 별도의 동의를 받아야 한다.

② 다른 법률에 특별한 규정이 있는 경우

다른 법률에 개인정보의 목적외 이용·제공에 대한 특별한 규정이 있는 경우에는 그에 따른 목적외 이용·제공이 허용된다.

'법률'로 한정되어 있으므로 시행령·시행규칙에만 관련 규정이 있는 경우에는 제2호에 따른 목적외 이용·제공이 허용되지 않는다. 다만 법률에 위임근거가 있고 이에 따라 시행령·시행규칙에 제공 관련 규정이 있는 경우는 허용된다. 또한 목적 외 이용·제공과 관련하여 '특별한 규정이 있는 경우'에 한하므로, '법령상 의무이행'과 같이 포괄적으로 규정된 경우도 역시 허용되지 않는다.

다른 법률의 특별한 규정 사례
● 소득세법 제170조에 따른 세무공무원의 조사, 질문 ● 감사원법 제27조에 따른 감사원의 자료 요구 ● 국가유공자 등 예우 및 지원에 관한 법률 제77조에 따른 국가보훈처장의 자료제공 요구 ● 병역법 제81조제2항에 따른 병무청장의 자료제공 요구 ● 부패방지 및 국민권익위원회 설치와 운영에 관한 법률 제42조제1항 및 제3항에 따른 국민권익위원회의 자료제출 요청 등

③ 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

명백히 정보주체 또는 제3자의 급박한 생명·신체·재산상의 이익을 위하여 필요하다고 인정되는 경우에는 정보주체의 별도 동의가 없더라도 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 명백히 정보주체 또는 제3자의 급박한 생명·신체·재산상의 이익을 위해 필요하다고 인정되는 경우임을 입증할 수 있어야 하며 관련 증빙을 보존하여야 한다.

④ 통계작성 및 학술연구 등의 목적

특정 개인을 알아볼 수 없는 형태로 편집 또는 가공해서 개인정보를 제공하는 경우에 한정된다. 이 경우 개인정보의 제공이 남용될 여지를 줄이기 위하여 제공하는 개인정보의 형태를 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

특정 개인을 알아볼 수 없는 형태로 편집 또는 가공 등 개인정보 비식별화 조치를 취했다 하더라도, 기술의 발전 및 외부 데이터와의 결합 등을 통해 재식별화 가능성이 높아질 수 있으므로, 비식별화 조치의 적정성을 충분히 검토하여 관련 위험을 최소화하는 것이 필요하다.

개인 식별요소 제거 요령 예시 (출처 : 공공정보 개방을 위한 개인정보보호 지침)	
처리 기법	주요 내용
가명처리 (pseudonymisation)	개인정보 중 주요 식별요소를 다른 값으로 대체하여 개인 식별을 곤란하게 함 (예) **홍길동, 35세,** 서울 거주, **한국대** 재학 → **임꺽정**, **30대** 서울 거주, **국제대** 재학 * 다른 값으로 대체하는 일정한 규칙이 노출되어 역으로 개인을 쉽게 식별할 수 있어서는 안된다.
총계처리 (Aggregation) 또는 평균값 대체(Replacement)	데이터의 총합값을 보임으로서 개별 데이터의 값을 보이지 않도록 함 (예) 임꺽정180cm, 홍길동170cm, 이콩쥐160cm, 김팥쥐150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm * 단, 특정 속성을 지닌 개인으로 구성된 단체의 속성 정보를 공개하는 것은 그 집단에 속한 개인의 정보를 공개하는 것과 마찬가지의 결과가 나타나므로 그러한 정보는 비식별화 처리로 볼 수 없음 (예〉 에이즈 환자 집단임을 공개하면서 특정인물 '갑'이 그 집단에 속함을 알 수 있도록 표시하는 것은 '갑'이 에이즈 환자임을 공개하는 것과 마찬가지임)

개인 식별요소 제거 요령 예시 (출처 : 공공정보 개방을 위한 개인정보보호 지침)	
처리 기법	주요 내용
데이터 값(가치) 삭제 (Data Reduction)	데이터 공유·개방 목적에 따라 데이터셋에 구성된 값 중에 필요없는 값 또는 개인식별에 중요한 값을 삭제 (예) 홍길동, 35세, 서울 거주, 한국대 졸업 → 35세, 서울 거주 (예) 주민등록번호 901206-1234567 → 90년대 생, 남자 (예) 개인과 관련된 날짜정보(자격취득 일자, 합격일 등)는 연단위로 처리 (예) 연예인·정치인 등의 가족 정보(관계정보), 판례 및 보도 등에 따라 공개되어 있는 사건과 관련되어 있음을 알 수 있는 정보
범주화 (Data Suppression)	데이터의 값을 범주의 값으로 변환하여 명확한 값을 감춤 (예) 홍길동, 35세 → 홍씨, 30-40세
데이터 마스킹 (data masking)	공개된 정보 등과 결합하여 개인을 식별하는데 기여할 확률이 높은 주요 개인식별자가 보이지 않도록 처리하여 개인을 식별하지 못 하도록 함 (예) 홍길동, 35세, 서울 거주, 한국대 재학 → 홍**, 35세, 서울 거주, **대학 재학) * 남아 있는 정보 그 자체로 개인을 식별할 수 없어야 하며 인터넷 등에 공개되어 있는 정보 등과 결합하였을 경우에도 개인을 식별할 수 없어야 한다.

⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보보호위원회의 심의·의결을 거친 경우

공공기관이 다른 법률에서 정하는 소관 업무를 수행하기 위하여 목적 외 이용 또는 제3자 제공이 불가피하게 필요한 경우가 있다. 그러나 소관 업무 수행이라는 목적 하에 개인정보 이용·제공을 무조건 허용하게 되면 남용의 소지가 많기 때문에 개인정보보호위원회의 심의·의결을 거치도록 하고 있다. 시행령·시행규칙에서 정하고 있는 소관업무로는 안 되고 반드시 '법률'에서 정하고 있는 업무이어야 한다. 다만 법률에 위임근거가 있고 이에 따라 시행령·시행규칙에 소관 업무가 규정된 경우는 허용된다.

⑥ 공공기관의 조약, 그 밖의 국제협정의 이행

「헌법」 제6조는 헌법에 의하여 체결, 공포된 조약과 일반적으로 승인된 국제법규는 국내법과 같은 효력을 가진다고 규정하고 있다. 조약이란 국가간의 문서에 의한 합의를 뜻하는데, 그 명칭이 조약이든, 조약 이외의 "협약, 협정, 규약, 선언, 의정서"이든 그 명칭 여하를 불문하고 '국가간의 문서에 의한 합의'이면 조약이 된다. 조약이 국내법과 동일한 효력을 가지면서 관련 규정이 상충할 때에는 특별법 우선적용의 원칙이 적용된다는 것이 일반적인 견해이다.

특별법은 일정한 사람·시간·장소에 대하여 그 효력이 미치는 것이므로, 조약의 체결시에는 조약의 체결 당사국이 조약규정을 그대로 적용하겠다는 의사합치가 있는 것으로 보아야 할 것이므로 조약에 대해 특별법적 지위를 인정할 수 있다. 따라서 법률의 효력을 가지는 조약이나 국제협정에서 개인정보의 목적외 이용 또는 제공을 규정하고 있다면, 이러한 조약 등의 이행을 위해서는 정보주체의 동의 없이도 개인정보를 목적 외 이용 또는 제공할 수 있다.

⑦ 공공기관의 범죄 수사와 공소의 제기 및 유지

개인정보처리자는 보유하고 있는 개인정보를 수집·이용 목적 이외의 용도로 제공하기 위해서는 다른 법률의 특별한 규정이 있거나 정보주체의 동의를 받아야 한다. 즉 공공기관 외의 개인정보처리자에 대해서는 비록 범죄수사 목적이라 하더라도 형사소송법 등의 규정에 따라서만 개인정보 제공을 요구할 수 있다.

그러나 공공기관의 경우 수사기관이 범죄수사, 공소제기 및 유지를 위해서 필요하다고 요청하는 경우 해당 개인정보를 정보주체의 별도의 동의 없이 제공할 수 있다. 이는 범죄수사편의를 위해 공공기관이 보유하고 있는 개인정보에 대해서는 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하기 위한 것이다.

범죄수사, 공소제기 및 유지를 위한 경우의 예외 및 한계 필요성
● 범죄수사, 공소제기·유지, 형집행 등의 형사절차에 「개인정보 보호법」을 그대로 적용할 경우, 수사기밀이 유출되거나 정보주체의 정보공개·정정요구 등으로 수사에 장애를 초래하여 범죄예방과 처단이 불가능해 질 우려가 있음 ● 수사가 종결되어 공소가 제기되면 정보주체는 법원에서 자유롭게 수사기록을 열람하여 자신의 정보를 확인하는 것이 가능하고, 불기소 처분된 경우는 정보공개청구를 통해 정보주체가 자신의 정보를 열람할 수 있으므로, 형사절차와 관련하여서는 「개인정보 보호법」 을 적용하지 아니하더라도 정보주체의 정보보호에 소홀한 점이 없음 ● 다만, 범죄수사등을 위한 경우라 하더라도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우에는 개인정보를 목적외의 용도로 이용하거나 제3자에게 제공할 수 없음

수사란 범죄의 혐의 유무를 명백히 하여 공소의 제기와 유지 여부를 결정하기 위하여 범인을 발견·확보하고 증거를 수집·보전하는 수사기관(검사, 사법경찰관리)의 활동을 발한다. 수사는 주로 공소제기 전에 하는 것이 일반적이나 공소제기 후에도 공소유지를 위하여 또는 공소유지여부를 결정하기 위한 수사도 허용된다.

「형사소송법」에 따라 검사는 범죄의 혐의가 있다고 사료되는 때에는 범인, 범죄사실과 증거를 수사하여야 하고(제196조), 검사의 지휘를 받아 사법경찰관리는 범죄의 혐의가 있다고 인식하는 때에는 범인, 범죄사실과 증거에 관하여 수사를 개시·진행한다(제197조). 수사는 수사기관의 주관적 혐의에 의해 개시되는데, 수사개시의 원인인 수사의 단서는 고소, 고발, 자수, 진정, 범죄신고, 현행범인의 체포, 변사자의 검시, 불심검문, 기사, 소문 등이 있다.

수사는 임의수사에 의하고 강제수사는 법률에 규정된 경우에 한하여 예외적으로 허용된다(「형사소송법」 제199조). 임의수사에는 공무소 등에 대한 조회(「형사소송법」 제199조제2항), 피의자신문(「형사소송법」 제200조 및 제241조 이하), 피의자 이외의 제3자에 대한 조사(「형사소송법」 제221조제1항제1문), 감정·통역·번역의 위촉(「형사소송법」 제221조제2항) 등이 있으며, 이러한 임의수사의 원칙은 임의수사자유의 원칙을 의미하는 것은 아니므로, 임의수사도 수사의 필요성과 상당성이 인정되어야만 적법한 수사라고 할 수 있다.

특히 임의수사를 위해 공무소 등에 조회를 하거나 공공기관에게 요청하는 자료에 개인정보가 포함되어 있다면 "범죄수사에 필요한 때"를 더욱 엄격히 해석함으로써 가능한 개인정보자기결정권에 대한 침해가 되지 않도록 해야 한다.

영장에 의하지 않는 경우에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 경우에 한하여 극히 제한적으로 개인정보를 제공하여야 할 것이며, 범죄의 형태나 경중, 정보주체가 받을 불이익의 정도 등 제반 사정을 종합적으로 고려하여 개인정보 이용이 없이는 수사의 목적을 달성할 수 없는 경우에 한하여 극히 제한적으로 개인정보를 제공하여야 할 것이다.

이와 관련하여 「신용정보법」 은 신용개인정보 제공의 근거를 법원이 발부한 영장에 두고 있으며, 영장을 발부받을 시간적 여유가 없을 급박한 경우에는 개인정보를 제공받은 이후에 검사는 영장을 청구하고, 36시간안에 영장을 받지 못한 경우에는 제공받은 개인정보를 폐기하도록 하고 있다.

⑧ 법원의 재판업무 수행

법원은 재판의 원활한 업무수행을 위해 공공기관이 보유하고 있는 개인정보에 대해 보정명령, 자료제출명령 등을 통해 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하고 있다.

⑨형(刑) 및 감호, 보호처분의 집행

형, 감호(보호감호, 치료감호), 보호처분의 원활한 집행을 위하여 공공기관이 보유하고 있는 개인정보의 목적 외 이용 또는 제공을 허용하고 있다.

- 수집한 개인정보를 수집목적의 범위를 벗어나 이용하기 위해서는 정보주체의 동의를 받아야 하며, 이때 ① 개인정보의 이용목적, ② 이용하는 개인정보의 항목, ③ 개인정보의 보유 및 이용기간, ④ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익에 관한 사항을 알려야 한다. 알려할 사항에 변경이 있는 때에도 이를 다시 알리고 동의를 받아야 한다.
- 수집·이용하고 있는 개인정보를 수집·이용 목적의 범위를 벗어나 제3자에게 제공하기 위해서는 정보주체의 동의가 필요하며, 이때 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭), ② 제공받는 자의 이용목적, ③ 제공하는 개인정보의 항목, ④ 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익을 정보주체에게 알려야 한다. 알려야 할 사항에 변경이 있는 때에도 이를 다시 알리고 동의를 받아야 한다.
- 공공기관이 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우에는 1개월 이내에 이용·제공의 법적 근거, 이용 또는 제공 일자·목적·항목에 관하여 관보 또는 인터넷 홈페이지에 게재하여 공고하여야 한다. 다만, 정보주체의 동의를 받거나 범죄수사와 공소제기 및 유지를 위해 개인정보를 목적 외로 이용하거나 제공하는 경우에는 그러하지 아니하다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.3.3	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 별도의 동의를 받거나 관련 법률에 근거하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○대학교는 AA업무에 대하여 경찰관직무집행법에 근거하여 제공하고 있으나, BB업무에서 졸업생 정보를 △△기관 제공하는 것은 별도의 법률에 규정되어 있지 않으므로 별도의 동의를 받아야 하나 받고 있지 않음				

평가업무명	제공근거	분석내용
AA업무	경찰관직무집행법 제8조	경찰관직무집행법에 규정하고 있음
BB업무	정보주체 별도 동의	정보주체에게 별도 동의 누락됨

OO법 제8조	경찰관 직무집행법 [시행 2017.7.26.] [법률 제14839호, 2017.7.26., 타법개정] 최종로그내용 제 영업시간이나 개방 장소가 불편인해서 범죄된 시간에 그 장소에 출입하였다고 보기에는 정당한 이유 없이 그 장구를 거절할 수 없다. ③ 경찰관은 대간접 직전 수행에 필요할 때에는 직전지역에서 제2항에 따른 장소를 감색할 수 있다. ④ 경찰관은 제1항부터 제3항까지의 규정에 따라 필요한 장소에 출입할 때에는 그 신분을 표시하는 증표를 제시하여야 하며, 함부로 관계인이 하는 정당한 업무를 방해해서는 아니 된다. [전문개정 2014.5.20.] 제8조(사실의 확인 등) ① 경찰관서의 장은 직무 수행에 필요하다고 인정되는 상당한 이유가 있을 때에는 국가기관이나 공사(公私) 단체 등에 직무 수행에 관련된 사실을 조회할 수 있다. 다만, 긴급한 경우에는 소속 경찰관으로 하여금 현장에 나가 해당 기관 또는 단체의 장의 협조를 받아 그 사실을 확인하게 할 수 있다. ② 경찰관은 다음 각 호의 직무를 수행하기 위하여 필요하면 관계인에게 출석하여야 하는 사유 일시 및 장소를 명확히 적은 출석 요구서를 보내 경찰관서에 출석할 것을 요구할 수 있다. 1. 미아를 인수할 보호자 확인 2. 유실물을 인수할 권리자 확인 3. 사고로 인한 사상자(死傷者) 확인 4. 행정처분을 위한 교통사고 조사에 필요한 사실 확인

관련법령 및 문서

관련 문서

【개인정보 보호법】

제18조(개인정보의 목적 외 이용 · 제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항 및 제39조의3제1항 및 제2항에 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, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)의 경우 제1호 · 제2호의 경우로 한정하고, 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. 삭제

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 보호위원회가 고시로 정하는 바에 따라 관보 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.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제18조

세부분야	목적 외 이용·제공 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.4	● **개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 이용목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?**		○		
평가 예시	● 미이행 : 일부 평가업무에서 목적외의 용도로 이용하거나 제3자 제공 시 최소한의 개인정보 항목으로 제한하고 있지 않는 경우				
평가근거 및 의견	● ○○대학교는 AA업무에 대하여 경찰관직무집행법에 근거하여 제공하는 경우, 최소한의 항목으로 제공하고 있으나, BB업무에서 졸업생정보를 △△기관 제공하는 경우 별도의 동의 없이 주민등록번호까지 제공하고 있음				

주요 점검 사항

1. 개인정보를 목적 외의 용도로 이용하거나 제공하는 경우, 이용 또는 제공되는 개인정보는 해당 목적에 맞는 최소한의 항목으로 제한하여야 한다.

지표 해설

- 3.3.3【지표 해설】참조
- 개인정보를 목적 외로 이용하거나 제공하는 경우에는 이용 또는 제공에 필요한 개인정보 항목을 정의하고 타당성을 검토한 후 업무수행에 필요한 최소한의 항목만을 이용하거나 제공하여야 한다.
- 정보주체의 동의를 받고 제3자에게 제공하는 경우라 할지라도, 최소 수집의 원칙에 따라 해당 제공목적에 필요한 최소한의 개인정보로 한정하는 것이 바람직하다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.3.4	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 이용목적에 맞는 최소한의 항목으로 제한하도록 계획하고 있습니까?		○		

평가근거 및 의견

● ○○대학교는 AA업무에 대하여 경찰관직무집행법에 근거하여 제공하는 경우, 최소한의 항목으로 제공하고 있으나, BB업무에서 졸업생정보를 △△기관 제공하는 경우 별도의 동의 없이 주민등록번호까지 제공하고 있음

평가업무명	제공근거	제공항목
AA업무	경찰관직무집행법 제8조	이름, 학과, 연락처
BB업무	정보주체 별도 동의	이름, 연락처, 주민등록번호, 주소

제3자 제공 대장에서의 제공되는 개인정보 항목

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭	학적파일		
이용 또는 제공 구분	[ ] 목적외 이용 [O] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)	-	담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)	- 경찰청	담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간	201		
이용하거나 제공한 형태	전자결재		
이용 또는 제공의 법적 근거	경찰관 직무집행법 제8조		
이용 목적 또는 제공받는 목적	수사지원		
이용하거나 제공한 개인정보의 항목	이름, 학과, 연락처		
「개인정보 보호법」 제18조제5항에 따라			

관련 문서

● 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제18조

세부분야	목적 외 이용·제공 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.5	● **개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 '개인정보 목적 외 이용 및 제공 대장'에 기록·관리하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : '개인정보 목적 외 이용 및 제3자 제공 대장'을 작성하나 일부 제공사항이 누락되거나, 기록한 내용이 미흡한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 제3자인 ○○○부에 개인정보를 매월 제공하고 있으며, 제공내역을 '개인정보 목적 외 이용 및 제3자 제공 대장'에 기록하여 관리하고 있음. 하지만 2019년 4월 제공내역을 기록하고 있지 않음				

주요 점검 사항

1. 개인정보를 목적 외의 용도로 이용하거나 제공하는 경우, '개인정보 목적 외 이용 및 제3자 제공 대장'에 관련 내용을 기록하고 관리해야 한다.
   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 개인정보보호를 위해 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용
2. 개인정보를 목적 외의 용도로 이용하거나 제공하는 경우, 제공 요청서, 결재 문서 등 관련 증적을 보관하고 관리해야 한다.

지표 해설

- 3.3.3, 3.3.4 【지표 해설】 참조
- 공공기관은 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 보호위원회가 정하여 고시하는 "개인정보의 목적 외 이용 및 제3자 제공 대장"에 기록하고 관리해야 한다.(「개인정보 보호법 시행령」 제15조)
  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

- 개인정보처리자가 개인정보를 목적 외로 제3자에게 제공할 때에는 개인정보를 제공받는 자가 개인정보를 안전하게 처리하도록 이용목적, 이용방법 등에 일정한 제한을 가하거나 제29조에 따른 안전성 확보조치를 강구하도록 요청하여야 한다.

  개인정보처리자는 제공과 동시에 또는 필요한 경우 제공한 이후에 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. 또한 이러한 사항은 "개인정보의 목적 외 이용 및 제3자 제공 대장"의 "8. 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용"에 기록하면 된다.(표준지침 제8조제2항)

- "개인정보의 목적 외 이용 및 제3자 제공 대장"은 「개인정보 처리 방법에 관한 고시」 별지 제1호 서식에 따라 작성되어야 한다.

■ 개인정보 처리 방법에 관한 고시 [별지 제1호서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의경우)		담당자	소 속
			성 명
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명
			소 속
			전화번호
이용하거나제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.3.5	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 '개인정보 목적 외 이용 및 제공 대장'에 기록·관리하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 제3자인 ○○○부에 개인정보를 매월 제공하고 있으며, 제공내역을 '개인정보 목적 외 이용 및 제3자 제공 대장'에 기록하여 관리하고 있음. 하지만 2013년 4월 제공내역을 기록하고 있지 않음.				

개인정보 목적 외 이용·제공 대장

개인정보 목적 외 이용.제공 대장

제공기관	제공일자	제공주기	제공형태	제공목적	제공근거	연계항목	비고
시스템	2013년 3월 4일	매월	DB를 시스템으로 온라인 연계함	XXXX 목적으로 OOOOO부로 송신함	OOO법 5조	이름, 주소, 교육일자, 교육비	건수 : 492255
시스템	2013년 5월 4일	매월	DB를 시스템으로 온라인 연계함	XXXX 목적으로 OOOOO부로 송신함	OOO법 5조	이름, 주소, 교육일자, 교육비	건수 : 403293

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법 시행령】

제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 보호위원회가 정하여 고시하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리해야 한다.

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

【개인정보 처리방법에 관한 고시】

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.

【표준 개인정보 보호지침】

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·제공 대장'에 기록하여 관리해야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제18조

세부분야	목적 외 이용·제공 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.6	● **개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 관련 내용을 관보 또는 인터넷 홈페이지 등을 통해 공개하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 대상시스템에서 취급하는 개인정보를 제3자 제공하는 경우 관련 사항을 개인정보 처리방침에 기재하고 인터넷 홈페이지·관보 등을 통하여 반영하도록 계획하고 있으나 안내사항의 일부만을 안내하는 경우				
평가근거 및 의견	● ○○시스템에서 취급하는 개인정보를 OO법에 의거 ○○업무 수행 목적으로 제3자 제공을 하고 있으며, 관련사항을 개인정보 처리방침에 기재하여 안내하고 있으나, 제공받는 기관, 제공하는 목적, 제공하는 항목 등을 안내하고 있으나, 제공근거, 제공일자 등이 명시되어 있지 않음				

주요 점검 사항

1. 개인정보를 목적 외의 용도로 이용하거나 제공하는 경우, 그 이용 또는 제공의 법적 근거, 목적 및 범위 등 관련 내용을 관보 또는 인터넷 홈페이지에 게재하여야 한다.

※ 단, 정보주체의 동의를 받았거나 범죄의 수사, 공소의 제기 및 유지를 위한 경우에는 제외됨

지표 해설

- 3.3.5【지표 해설】참조
- 공공기관이 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우에는 1개월 이내에 목적 외 이용·제공의 법적 근거, 이용 또는 제공 일자·목적·항목에 관하여 관보 또는 인터넷 홈페이지에 게재하여 공고하여야 한다. 다만, 정보주체의 동의를 받거나 범죄수사와 공소제기 및 유지를 위해 개인정보를 목적 외로 이용하거나 제공하는 경우에는 그러하지 아니하다.

개인정보의 목적 외 이용 및 제3자 제공 내용 홈페이지·관보 등 게재 사항
● 목적 외 이용 등을 한 날짜 ● 목적 외 이용 등의 법적 근거 ● 목적 외 이용 등의 목적 ● 목적 외 이용 등을 한 개인정보의 항목

평가 예시

<table>
<tr><th>구 분</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>3.3.6</td><td>개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 관련 내용을 관보 또는 인터넷 홈페이지 등을 통해 공개하도록 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가근거 및 의견</td><td colspan="5">● ○○기관은 '공공기관 고객만족도 조사'에 대한 자료로서 고객 정보를 상급기관에 법률에 근거하여 제공을 하였으나, 제공한 사실에 대한 날짜, 제공 근거를 안내하지 않고, 개인정보파일명칭도 운영 중인 개인정보 파일명과 일치하지 않음.
<table>
<tr><td rowspan="3">홈페이지 (개인정보의 제3자 제공 현황)</td><td colspan="5"><table>
<tr><th>개인정보 파일명</th><th>제공 받는 자</th><th>제공목적</th><th>제공 항목</th><th>보유 및 이용기간</th></tr>
<tr><td>공공기관 청렴도 측 정대상 파일</td><td>국민권익 위원회</td><td>공공기관 청렴도 평가를 위한 민원인, 정책고객, 직원에 대한 설문조사 실시</td><td>성명, 전화번호, 이메일, 주소</td><td>목적달성 시 까지</td></tr>
<tr><td>○○○ 자격증 진위 여부</td><td>○○○ 기관</td><td>○○ 기술자격 검정항목 면제를 위한 자격증명서 진위여부 확인</td><td>○○○ 자격증 진위 여부</td><td>목적달성 시 까지</td></tr>
</table></td></tr>
</table></td></tr>
</table>

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제18조(개인정보의 이용·제공 제한)

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 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

【개인정보 처리방법에 관한 고시】

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

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제18조

세부분야	목적 외 이용·제공 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.3.7	● **개인정보를 제3자에게 제공하거나 연계하는 경우 암호화 조치, 보유기간 지정 등 안전성 확보를 위해 필요한 조치를 적용하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 개인정보를 타 기관에 연계·제공 시 안전성 확보조치를 적용하지 않은 경우				
평가근거 및 의견	● ○○연수원의 ○○팀 담당자는 A기관 ○○팀 담당자로부터 ○○법에 의거 수강생들의 연수현황 등 개인정보 제공에 대하여 구두요청을 하였으며, 담당자는 별도의 문서요청 없이 A기관 ○○팀 담당자에게 수강생들의 연수현황 등이 담긴 개인정보를 제공하였음				

주요 점검 사항

1. 개인정보를 제3자에게 제공하는 경우, 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 보유 기간, 그 밖에 필요한 사항에 대해 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 공식적으로 요청하여야 한다.
   ※ 목적 외 제공 여부, 법률에 근거한 제공 여부 등에 따라 필요한 조치의 수준 및 방법이 상이할 수 있음(목적 외 제공일 경우에는 법적 필수 사항, 목적 내 제공일 경우에는 권고 사항)
2. 개인정보를 제3자에게 제공하는 경우, 사후에 확인이 가능하도록 관련 기록을 남기고 보존하여야 한다.
3. 개인정보를 제3자에게 제공하거나 연계하는 과정에서의 개인정보 유·노출, 변조, 훼손 등을 방지하기 위하여, 전용선 또는 VPN 등의 안전한 전송 수단을 적용하거나 암호화, 접근제어 등 안전성 확보를 위해 필요한 조치를 적용하여야 한다.

지표 해설

- 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다. (표준지침 제8조제2항)
- 개인정보처리자가 개인정보를 목적 외의 용도로 제3자에게 제공할 때에는 개인정보를 제공받는 자가 개인정보를 안전하게 처리하도록 이용목적, 이용방법 등에 일정한 제한을 가하거나 제29조에 따른 안전성 확보조치를 강구하도록 요청하여야 한다. 개인정보처리자는 제공과 동시에 또는 필요한 경우 제공한 이후에 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.(「개인정보 보호법」 제18조제5항, 표준지침 제8조제1항)

개인정보 보호법 제29조에 따른 안전성 확보조치
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

- 개인정보를 목적 외로 제3자에게 제공하는 경우가 아니라 하더라도, 개인정보를 제3자에게 제공하게 될 때는 제3자로 인한 개인정보 침해사고가 발생할 경우 제공자에게도 민원이 발생하거나 함께 조사를 받게 되는 등의 리스크가 있을 수 있다. 따라서, 개인정보를 제3자에게 제공하는 과정에서 개인정보가 유·노출 및 훼손·변조 되거나 제3자에 의해 오남용되지 않도록 안전성 확보 조치를 적용하는 등 정당한 주의 의무 관점에서 적절한 조치를 취하는 것이 바람직하다.(권고사항)

- 공개된 인터넷망을 통하여 개인정보를 제공하는 경우에는 전용망 또는 가상사설망(VPN) 등 안전한 전송수단 적용이 필요하나, 불가피 하게 적용이 어려운 경우에는 별도의 암호화 조치 등을 통해 전송 과정에서의 개인정보 유·노출, 변조, 훼손 등을 방지하는 것이 필요하다.
  ※ 고유식별정보, 비밀번호, 바이오정보 이외의 개인정보도 공개망으로 송·수신 하는 경우 암호화 권고
  ※ 다양한 연계방식에 따른 적절한 보안조치 필요 (예를 들어, 평가대상기관에서 개인정보처리시스템의 권한을 열어주고 제공받는 자가 접속하여 받아가는 경우 계정관리, 권한관리, 접근제어, 접속기록 점검 등의 보호조치 적용 등)

- 공공기관의 경우 외부기관과의 개인정보 연계·제공을 위하여 온라인으로 개인정보를 전송하는 경우 정부고속망 등의 전용망 또는 행정정보중계시스템의 이용을 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.3.7	개인정보를 제3자에게 제공하거나 연계하는 경우 암호화 조치, 보유기간 지정 등 안전성 확보를 위해 필요한 조치를 적용하도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○기관은 이용자의 개인정보를 정보주체의 별도 동의를 받아 제휴몰사에 상품홍보를 위한 목적으로 개인정보를 제공하며, 제공 시 A제휴몰사 ○○시스템에 접근하여 이용자의 개인정보가 담긴 리스트파일을 업로드하고 있으나, ○○시스템은 SSL 등 전송 시 암호화가 되어 있지 않으며, 붙임파일 또한 파일 암호화가 되어 있지 않음. [개인정보 제공(전송) 시 암호화 미적용] 				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제18조(개인정보의 이용·제공 제한)

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

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.

【개인정보 보호법 시행령】

제30조(개인정보의 안전성 확보조치)

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

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제18조
- 개인정보의 안전성 확보조치 기준 해설서

4 위탁

세부분야	개인정보 제공의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.4.1	● **개인정보 처리에 관한 업무 위탁 시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 대상시스템에서 취급하는 개인정보 처리업무에 대하여 위탁·위임하는 경우 관련 사항을 개인정보 처리방침에 기재하고 인터넷 홈페이지·관보 등을 통하여 반영하도록 계획하고 있으나 일부만을 공개하는 경우				
평가근거 및 의견	● A기관은 ○○시스템의 유지보수 및 운영에 관한 업무를 B기관에 위탁을 하고, 고객의 상품 마케팅 홍보 업무를 C업체에 위탁하고 있으나, 이 중 상품 마케팅 홍보 업무에 관한 위탁업무를 안내하고 있지 않음				

주요 점검 사항

1. 개인정보의 처리업무를 제3자에게 위탁하는 경우, 관련 사항을 정보주체가 쉽게 확인할 수 있도록 '개인정보 처리방침' 등을 통해 지속적으로 공개해야 한다.
   ① 위탁하는 업무의 내용
   ② 개인정보 처리업무를 위탁받아 처리하는 자(수탁자)
   ※ 모든 수탁자가 빠짐없이 공개되어야 함
2. 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 정보주체에게 관련 사항을 명시적으로 알려야 한다.

지표 해설

- 업무위탁의 유형은 크게 개인정보의 수집·관리 업무 그 자체를 위탁하는 개인정보처리업무 위탁과 개인정보의 이용·제공이 수반되는 일반 업무를 위탁하는 개인정보취급업무 위탁으로 구분될 수 있다. 또한 개인정보취급업무 위탁은 다시 홍보·판매권유 등 마케팅업무의 위탁과 상품배달·애프터서비스 등 계약이행업무의 위탁으로 구분할 수도 있다.
- 개인정보 처리 업무를 위탁하는 개인정보처리자(위탁자)는 ① 위탁하는 업무의 내용과 ② 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 자신의 인터넷 홈페이지(개인정보 처리방침)에 지속적으로 게재하는 방법으로 공개하여야 한다.
- 위탁자가 위탁업무의 내용, 수탁자의 이름 등을 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 공개하여야 한다.

위탁업무 등의 공개방법
1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법 2. 관보(위탁자가 공공기관인 경우로 한정한다)나 위탁자의 사업장등이 소재하는 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 · 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법 3. 동일한 제호로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물 · 소식지 · 홍보지 · 청구서 등에 지속적으로 싣는 방법 4. 재화 또는 용역을 제공하기 위한 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

- 이때 개인정보 처리업무와 관련된 수탁자는 누락 없이 공개가 되어야 한다. 수탁자수가 매우 많아 개인정보 처리방침 내에서 모두 표시하는 것이 어려운 경우에는 별도의 링크를 통해 전체 수탁자를 조회할 수 있도록 하는 것도 가능하다.
- 신규 수탁자와의 계약 또는 기존 수탁자와의 계약 해지 등으로 수탁자의 변경이 발생한 경우에는 지체 없이 관련 내용을 개인정보처리방침 등에 반영하여 공개하여야 한다. 일반적으로 이러한 변경사항이 제대로 반영되지 않는 경우가 많으므로 수탁사와의 계약 체결·해지 절차 상에 관련 절차를 마련하거나 정기적으로 수탁자 현황을 조사하여 반영하는 절차를 가져갈 필요가 있다.
- 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 모사전송, 전화, 문자전송 또는 이에 상당하는 방법으로 ①위탁하는 업무의 내용과 ②수탁자를 정보주체에게 알려야 한다. 위탁자가 과실 없이 서면, 전자우편 등이 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 않는 위탁자의 경우에는 사업장 등 보기 쉬운 장소에 30일 이상 게시하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.4.1	개인정보 처리에 관한 업무 위탁 시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하도록 계획하고 있습니까?		○		

평가근거 및 의견

● A기관은 ○○시스템의 유지보수 및 운영에 관한 업무를 B기관에 위탁을 하고, 고객의 상품 마케팅 홍보 업무를 C업체에 위탁하고 있으나, 이 중 상품 마케팅 홍보 업무에 관한 위탁업무를 안내하고 있지 않음

수탁사	위탁내용	분석내용
B기관	시스템 유지보수 및 운영	개인정보처리방침에 공개
C업체	고객상품 마케팅 홍보 업무	개인정보처리방침에 공개되지 않음

○○○ 회원정보 (개인정보 처리 방침)

제4조 개인정보처리 위탁

① [redacted]는 원칙적으로 이용자의 동의없이 해당 개인정보의 처리를 타인에게 위탁하지 않습니다. 다만, 광고 등이 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 「개인정보보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)에 따라 다음 각 호의 내용이 포함된 문서에 의하여 위탁하여, 위탁 업무의 내용과 수탁자를 [redacted] 홈페이지에 게시합니다.

가. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

나. 개인정보의 관리적 기술적 보호조치에 관한 사항

다. 개인정보의 안전관리에 관한 사항

- 위탁업무의 목적 및 범위, 재 위탁 제한에 관한 사항, 개인정보 안전성 확보 조치에 관한 사항, 위탁업무와 관련하여 보유하고 있는 개인정보의 관리현황점검 등 감독에 관한 사항, 수탁자가 준수하여야할 의무를 위반한 경우의 손해배상책임에 관한 사항

② 한국기술사회는 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

수탁업체	위탁업무내용	개인정보의 보유 및 이용기간
KISTI	사업운영	회원탈퇴 시 혹은 위탁계약 종료시까지
KI	통합 시스템 운영 및 유지보수	회원탈퇴 시 혹은 위탁계약 종료시까지

③ 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제26조(업무위탁에 따른 개인정보의 처리 제한)

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.

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)

   3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
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

【개인정보 보호법 시행령】

제28조(개인정보의 처리 업무 위탁시 조치)

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.

제31조(개인정보 처리방침의 내용 및 공개방법 등)

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

【표준 개인정보 보호지침】

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

6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제26조

세부분야	위탁 계약				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.4.2	● **개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보 관리에 관한 책임사항이 위탁계약서에 일부만 포함되거나 일부 위탁기관에 대해서만 위탁계약서를 작성한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 ○○업무를 위해 '○○○ 업체'와 위탁계약을 맺고 위탁계약서를 작성하였으나 위탁계약서의 필수 요건 중 '개인정보의 관리 현황 점검'에 대한 사항이 누락되어 있음				

주요 점검 사항

1. 개인정보의 처리업무를 제3자에게 위탁하는 경우, 아래 사항이 포함된 문서에 의하여야 한다.
   ① 위탁업무 수행 목적 외 개인정보 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

지표 해설

- 업무위탁과 개인정보 제3자 제공 모두 개인정보가 다른 사람에게 이전하거나 다른 사람과 공동으로 이용하게 된다는 측면에서는 동일하지만 개인정보 이전의 목적이 전혀 다르고 이전된 개인정보에 대한 관리·감독 등 법률적 관계도 전혀 다르다.
- 업무위탁의 경우에는 개인정보처리자의 업무처리 범위 내에서 개인정보 처리가 행해지고 위탁자인 개인정보처리자의 관리·감독을 받지만, 제3자 제공은 제3자의 이익을 위해서 개인정보 처리가 행해지고 제3자가 자신의 책임 하에 개인정보를 처리하게 된다. 따라서 업무위탁의 경우에는 수탁자에게 개인정보가 이전되더라도 개인정보에 대한 개인정보처리자의 관리·감독권이 미치지만, 제3자 제공의 경우에는 일단 개인정보가 제3자에게 제공되고 나면 개인정보처리자의 관리·감독권이 미치지 못한다.

업무 위탁과 제3자 제공의 비교		
구분	업무위탁	제3자 제공
관련조항	제26조	제17조
예시	· 배송업무 위탁, TM 위탁 등	· 사업제휴, 개인정보 판매 등
이전목적	· 위탁자의 이익을 위해 처리(수탁업무 처리)	· 제3자의 이익을 위해 처리
예측 가능성	· 정보주체가 사전 예측 가능 (정보주체의 신뢰 범위내)	· 정보주체가 사전 예측 곤란 (정보주체의 신뢰 범위 밖)
이전 방법	· 원칙 : 위탁사실 공개 · 예외 : 위탁사실 고지(마케팅 업무위탁)	· 원칙 : 제공목적 등 고지 후 정보주체 동의 획득
관리·감독책임	위탁자 책임	제공받는 자 책임
손해배상책임	위탁자 부담(사용자 책임)	제공받는 자 부담

- 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

위탁업무 문서화 내용
1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항(법 제26조제1항) 2. 개인정보의 기술적·관리적 보호조치에 관한 사항(법 제26조제1항) 3. 위탁업무의 목적 및 범위(시행령 제28조제1항) 4. 재위탁 제한에 관한 사항(시행령 제28조제1항) 5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항(시행령 제28조제1항) 6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항(시행령 제28조제1항) 7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항(시행령 제28조제1항)

[위탁계약서 샘플]

표준 개인정보처리위탁 계약서(안)

○○○(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 "위탁자"가 개인정보처리업무를 "수탁자"에게 위탁하고, "수탁자"는 이를 승낙하여 "수탁자"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 「개인정보 보호법」, 같은 법 시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호) 및 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "수탁자"는 계약이 정하는 바에 따라 (　　) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다. 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

1.
2.
3.

제4조 (위탁업무 기간) ① 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.
계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① "수탁자"는 "위탁자"의 사전 승낙을 얻은 경우를 제외하고 "위탁자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② "수탁자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "수탁자"는 해당 사실을 계약 체결 7일 이전에 "위탁자"에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) "수탁자"는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "수탁자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② "수탁자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호)에 따라 즉시 파기하거나 "위탁자"에게 반납하여야 한다.
③ 제2항에 따라 "수탁자"가 개인정보를 파기한 경우 지체없이 "위탁자"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "위탁자"는 "수탁자"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "수탁자"는 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 "위탁자"는 "수탁자"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이행하여야 한다.
③ "위탁자"는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 ( )회 "수탁자"를 교육할 수 있으며, "수탁자"는 이에 응하여야 한다. 「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2020-2호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.
④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "위탁자"는 "수탁자"와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "수탁자"는 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "수탁자"는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "위탁자"에게 확인받아야 한다.

제11조 (손해배상) ① "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "위탁자" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "수탁자"는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "위탁자"가 전부 또는 일부를 배상한 때에는 "위탁자"는 이를 "수탁자"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "위탁자"와 "수탁자"가 서명 또는 날인한 후 각 1부씩 보관한다.

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)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.4.2	개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 XXX를 위해 '○○○ 업체'와 위탁계약을 맺고 위탁계약서를 작성하였으나 위탁계약서의 필수 요건 중 '개인정보의 관리 현황 점검'에 대한 사항이 누락되어 있음.				

개인정보 처리 위탁계약 추가 특수조건	**개인정보처리 위탁계약 추가특수조건** 이 개인정보처리 위탁계약 추가특수조건(이하 "추가특수조건"이라 한다)은 [ ] (이하 "갑"이라 한다)과 (이하 "을"이라 한다)간에 개인정보처리 위탁계약 이행에 대한 계약조건을 정함을 목적으로 하며, 이 추가특수조건에 의거 신의와 성실의 원칙에 따라 계약을 이행하여야 한다. **제1조 (목적)** 이 추가특수조건은 "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 추가특수조건에서 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 과업내용서 등 계약이 정하는 바에 따라 개인정보 처리 업무를 수행한다. **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.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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

【개인정보 보호법 시행령】

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

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제26조
- 표준 개인정보처리위탁 계약서(샘플)

세부분야	위탁 계약				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.4.3	● **개인정보 처리에 관한 업무를 위탁받아 처리하는 자(수탁자)를 대상으로 개인정보 보호 교육, 처리현황 점검 등 관리·감독 활동을 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 수탁자에 대한 관리·감독 계획이 수립되어 있으나, 교육계획 등 일부 사항이 누락되어 있는 경우 또는 현장 실태점검 계획 없이 수탁자 자체점검 계획만 존재하는 경우				
평가근거 및 의견	● ▲▲▲ 기관은 '2015년 개인정보 수탁사 점검 계획'에 따라 2015년 6월에 실태점검을 수행하였으나, 전체 수탁사 10개 중 2개사(○○○, △△△)에 대해서는 실태점검이 수행되지 않음				

주요 점검 사항

1. 개인정보 처리업무를 위탁받아 처리하는 자(수탁자)를 대상으로 아래 사항을 포함한 관리·감독 계획을 수립하고 이에 따라 관리·감독 활동을 수행하여야 한다.
   ① 개인정보보호 서약서 작성
   ② 개인정보보호 교육 시행
   ③ 정기적인 실태 점검
   ④ 기타 수탁자 관리·감독을 위해 필요한 활동

지표 해설

- 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지 감독하여야 한다.
- 또한 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위· 수탁 계약(법 제26조 제1항 각 호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다(영 제28조 제6항)
- 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자 소속 직원 중 개인정보취급자에 대해서는 개인정보보호 서약서를 작성하도록 하고, 수탁자의 개인정보처리 현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 접근권한 관리 등 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.
- 수탁자가 자체적으로 실태 점검을 수행한 후에 점검 결과를 제출하도록 하는 방법도 가능하지만, 전적으로 수탁자 자체점검에 의존하는 것은 바람직하지 않으며 정기적인 현장 점검을 통하여 자체 점검이 적절하게 수행되고 있는지 확인할 필요가 있다.
- 실태 점검을 통해 발견된 문제점에 대해서는 조치가 될 수 있도록 관리 절차를 마련하여 지속적으로 관리하여야 한다.
- 수탁자에 대한 관리·감독 활동은 1회성이 아니라 지속적으로 수행되어야 하며, 이를 위해서는 일시, 대상, 내용(방법론), 점검 기준(체크리스트), 담당자 등을 포함한 수탁자 관리·감독 및 점검 계획을 수립·시행하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.4.3	개인정보 처리에 관한 업무를 위탁받아 처리하는 자(수탁자)를 대상으로 개인정보 보호 교육, 처리현황 점검 등 관리·감독 활동을 계획하고 있습니까?		○		

평가근거 및 의견

- ▲▲▲ 기관은 '2015년 개인정보 수탁사 점검 계획'에 따라 2015년 6월에 실태점검을 수행하였으나, 전체 수탁사 10개 중 2개사(○○○, △△△)에 대해서는 실태점검이 수행되지 않음
- 8개 점검한 수탁사 대상으로 개인정보보호 교육, 개인정보보호 서약서, 개인정보의 안전한 관리 등을 조사하였음

2015년 개인정보 수탁사 실태점검 결과

3. 점검 대상 수탁사

번호	수탁사 명	점검 일시	점검 결과
1	○○정보통신	2015.05.04	양호
2	△△테크	2015.05.04	양호
3	□□□용역	2015.05.06	보통
4	○○○모바일	2015.05.06	양호
5	◎◎서비스	2015.05.10	양호
6	ⓘⓘⓘⓘ정보	2015.05.10	양호
7	◇◇파트너스	2015.05.11	양호
8	◉◉비즈니스	2015.05.11	미흡

개인정보보호 교육 이수자 명단 통보

구분	부서(조직명)			교육명	교육기간	교육시간
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁부서	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시
위탁업체	[redacted]	[redacted]	2015[redacted]	상시학습 교육	2015.7.24(금)	3시

보안서약서(용역업체 직원용)

[redacted]

20[redacted] 년 [redacted] 월 [redacted] 일

[redacted]

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제26조(업무위탁에 따른 개인정보의 처리 제한)

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.

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.

【개인정보 보호법 시행령】

제28조(개인정보의 처리 업무 위탁시 조치)

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.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제26조

5 파기

세부분야	파기 계획 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.5.1	● **개인정보의 보유 목적이 달성되었거나 보유 기간이 경과되었을 때 지체 없이 파기되도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보파일의 법률에 근거한 보유기간 산정이 일부 잘못 되었거나, 파기는 수행되고 있으나 일부는 파기되지 않고 보존하고 있는 경우				
평가근거 및 의견	● 9개의 개인정보파일 중 5개의 개인정보파일은 보존기간 종료 시 지체 없이 파기되고 있었으나, 4개 파일(○○파일, ○○파일, ○○파일, ○○파일)은 서류 문서만 파기하고 DB내 개인정보는 미파기됨				

주요 점검 사항

1. 개인정보의 보유기간 경과, 처리목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.
   ① 개인정보의 보유 기간 경과
   ② 개인정보의 처리목적 달성
   ③ 법령에 따라 보존하고 있는 경우, 그 보존 기간 경과
   ※ 단, 다른 법령에 따라 보존해야 하는 경우에는 그러하지 아니함
   ※ 파기시 복구·재생되지 않도록 안전하게 파기하여야 함(지표번호 4.7.1)

지표 해설

- 본 지표에서는 개인정보 흐름분석 결과를 바탕으로 개인정보파일별로 목적 달성 또는 보유기간 경과 시 지체없이 파기하는지 여부를 평가한다. 개인정보처리시스템 구축단계에서는 파기여부를 직접적으로 확인할 수 없으므로, DB 및 시스템 설계 상에 개인정보 파기에 대한 기준 및 로직이 적절히 반영되었는지를 점검하여야 한다.
- 개인정보를 수집했던 목적이 달성되어 보존 필요성이 없어졌는데도 이를 계속해서 보유할 경우 개인정보의 유출과 오용 가능성이 높아지므로 더 이상 개인정보가 불필요하게 된 때에는 이를 파기시킴으로써 개인정보를 안전하게 보호하려는 것이다.
- 개인정보처리자가 개인정보 보유기간을 고지하고 동의 받는 경우 그 보유기간을 정할 때에는 그 보유목적이 명백히 영구히 보유하여야 하는 경우에는 영구, 그렇지 않은 경우 필요 최소한으로 정해야 한다. 이 경우 입증책임은 개인정보처리자가 부담한다.

- 개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기해야 한다. “개인정보가 불필요하게 되었을 때”란 개인정보의 처리목적이 달성되었거나, 해당 서비스의 폐지, 사업의 종료된 경우 등이 포함된다. 따라서 개인정보처리자는 처리목적이 달성되거나, 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한, 5일 이내에 개인정보를 파기하여야 한다.(표준지침 제10조제1항) 개인정보의 보존 필요성이 있는지 여부는 객관적으로 판단하여야 하며 자의적으로 해석해서는 안 된다.

개인정보가 불필요하게 되었을 때(예시)
● 개인정보처리자가 당초 고지하고 동의를 받았던 보유기간의 경과 ● 동의를 받거나 법령 등에서 인정된 수집·이용·제공 목적의 달성 ● 회원탈퇴, 제명, 계약관계 종료, 동의철회 등에 따른 개인정보처리의 법적 근거 소멸 ● 개인정보처리자의 폐업·청산 ● 대금 완제일이나 채권소멸시효기간의 만료

- 개인정보를 파기할 때에는 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기하여야 한다. 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기적으로 기록된 개인정보는 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 하여야 하며, 종이와 같이 출력물의 형태로 되어 있는 경우에는 물리적으로 분쇄하거나 소각하는 방법으로 해당 개인정보를 완전히 파기하여야 한다. (지표번호 4.7.1 참고)
- 개인정보처리자는 개인정보의 파기에 관한 사항을 기록하고 관리하여야 한다. 보유목적을 달성한 개인정보의 파기는 법적 의무사항이며 위반 시 벌칙이 부과되는 사항이므로 파기는 반드시 개인정보 보호책임자의 책임 하에 수행되어야 하며, 개인정보 보호책임자는 파기 결과를 확인하여야 한다.(표준지침 제10조 제3항부터 제5항)
- 개인정보처리자는 ‘다른 법령에 따라 보존해야 하는 경우’에는 예외적으로 개인정보를 파기하지 않아도 된다. 개인정보처리자가 개인정보를 파기하지 않고 보존하려고 하는 경우에는 그 법적 근거를 명확히 해야 한다. 채권소멸기간까지 개인정보를 보존할 수 있다고 하여 이미 요금정산이 끝난 소비자의 개인정보까지 보존하여서는 안 된다. 신용카드 이용고객의 신용관리를 이유로 회원의 동의 없이 탈퇴회원의 개인정보를 일정기간 보존하는 것도 파기의무 위반이다. 다른 법령에서 보존기간으로 정한 기간이 만료한 경우에는 지체 없이 파기하여야 한다.

보존의무를 규정하고 있는 입법례
「전자상거래 등에서의 소비자보호에 관한 법률」 및 동법 시행령(제6조) ① 법 제6조제3항에 따라 사업자가 보존하여야 할 거래기록의 대상 · 범위 및 기간은 다음 각 호와 같다. 다만, 법 제20조제1항에 따른 통신판매중개자(이하 "통신판매중개자"라 한다)는 자신의 정보처리시스템을 통하여 처리한 기록의 범위에서 다음 각 호의 거래기록을 보존하여야 한다. 1. 표시 · 광고에 관한 기록: 6개월 2. 계약 또는 청약철회 등에 관한 기록: 5년 3. 대금결제 및 재화등의 공급에 관한 기록: 5년 4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년 **「통신비밀보호법」 제15조의2 및 동법 시행령 제41조** ② 법 제15조의2제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다. 1. 법 제2조제11호가목부터 라목까지 및 바목에 따른 통신사실확인자료 : 12개월. 다만, 시외 · 시내전화역무와 관련된 자료인 경우에는 6개월로 한다. 2. 법 제2조제11호마목 및 사목에 따른 통신사실확인자료 : 3개월 **「의료법」 시행규칙 제15조** ① 환자 명부 : 5년 ② 진료기록부 : 10년 ③ 처방전 : 2년 ④ 수술기록 : 10년 ⑤ 검사소견기록 : 5년 ⑥ 방사선사진 및 그 소견서 : 5년 ⑦ 간호기록부 : 5년 ⑧ 조산기록부: 5년 ⑨ 진단서 등의 부본 (진단서·사망진단서 및 시체검안서 등을 따로 구분하여 보존할 것) : 3년

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.5.1	개인정보의 보유 목적이 달성되었거나 보유 기간이 경과되었을 때 지체 없이 파기되도록 계획하고 있습니까?		○		

평가근거 및 의견

● 9개의 개인정보파일 중 5개의 개인정보파일은 보존기간 종료 시 지체 없이 파기되고 있었으나, 4개 파일(○○파일, ○○파일, ○○파일, ○○파일)은 서류 문서만 파기하고 DB내 개인정보는 미파기됨

평가업무	파일명	분석내용
A평가업무	A파일	파기수행 됨
B평가업무	○○파일	문서만 파기되고, DB는 파기되지 않음
C평가업무	C파일	파기수행 됨
D평가업무	D파일	파기수행 됨
E평가업무	○○파일	문서만 파기되고, DB는 파기되지 않음
F평가업무	○○파일	문서만 파기되고, DB는 파기되지 않음
G평가업무	○○파일	문서만 파기되고, DB는 파기되지 않음
H평가업무	H파일	파기수행 됨
I평가업무	I파일	파기수행 됨

개인정보 파일 보유기간 및 파기 수행여부

시스템명	개인정보파일명	보존기간	관리부서	파기담당부서	파기현황
	세파일	5년			문서 파기 DB 삭제
	일	3년	간	단	문서 파기 DB삭제 미진행
	일	3년	간	실	문서 파기 DB파기 미진행
시스템	일	5년	니	실	문서 파기 DB파기 미진행
	일	30년	니	실	문서 파기 DB파기 미진행
	파일	산정필요	니	실	DB파기 미진행
	일	산정필요	니	실	DB파기 미진행
	리파일	산정필요	니	실	DB파기 미진행
	일	3년	니	실	0건

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【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 보호위원회가 정하여 고시한다.

【표준 개인정보 보호지침】

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 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제21조

세부분야	분리보관 계획 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.5.2	● **다른 법령 등에 따라 개인정보를 보존할 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장 · 관리 하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 이용 목적을 달성한 개인정보를 다른 개인정보와 분리하여 보관하도록 계획하고 있지 않은 경우				
평가근거 및 의견	● ○○시스템 회원정보 중 탈퇴한 회원정보는 통계목적을 위해 해당 테이블에 그대로 Disable 상태로 보존하고 있음				

주요 점검 사항

1. 개인정보의 보유기간 경과, 처리목적 달성 등으로 인하여 파기하여야 함에도 불구하고, 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 한다.
2. 분리 보관된 개인정보는 보존 근거가 되는 법령 상 필요한 경우에만 접근할 수 있도록 접근권한 분리, 접속기록 보관, 접근 통제 등의 보호조치가 적용되어야 한다.

지표 해설

- 3.5.1 【지표 해설】 참조
- 개인정보처리자는 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다. 이를 위해 물리적 또는 논리적으로 분리된 시스템(DB 등)에 별도로 보관하는 방법을 사용하여야 한다.
- 미파기 정보가 기존 개인정보와 혼재되어 있다면, 예를 들어 회원들을 대상으로 한 메일 발송 시 탈퇴 회원에게도 같이 발송되는 경우와 같이 개인정보의 목적 외 이용이나 유출, 오·남용의 위험성이 커지므로 이를 방지하기 위한 규정이다. 미파기 정보는 오로지 다른 법령에서 보존하도록 한 목적 범위 내에서만 처리 가능하도록 관리되어야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.5.2	다는 법령 등에 따라 개인정보를 보존할 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장 · 관리하도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○시스템 회원정보 중 탈퇴한 회원정보는 통계목적을 위해 해당 테이블에 그대로 Disable 상태로 보존하고 있음				

회원DB내 회원 정보 Table	

No.		아이디	사용자이름	사용자이메일	전화번호	등록일	가입상태
1		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-18	회원가입삭제
2		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-17	회원가입신청
3		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-17	회원탈퇴
4		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-17	회원가입신청
5		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-17	회원가입신청
6		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-17	회원가입신청
7		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-16	회원가입승인
8		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-16	회원탈퇴
9		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-14	회원가입신청
10		[redacted]	[redacted]	[redacted]	[redacted]	2009-04-08	회원가입승인

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

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

관련 문서

● 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제21조

세부분야	분리보관 계획 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
3.5.3	● **개인정보파일을 파기하는 경우 파기 결과 등을 '개인정보파일 파기 관리대장'에 기록·관리하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보파일 파기 관리대장을 문서로 관리하고 있으나 일부 파기 사실이 누락되거나, 기록한 파기내용이 미흡한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '○○○ 발송 정보', '○○○ 위원 현황' 등 5건의 개인정보 파기 사실이 있어 4건에 관해서는 '개인정보 파기 대장'에 기록하였으나 'XXX 현황'에 대한 파기 사실은 누락되어 있음				

주요 점검 사항

1. 공공기관은 개인정보파일의 보유기간 경과, 처리목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다.
2. 개인정보파일을 파기하는 경우, '개인정보파일 파기 관리대장'을 작성하여 관리하여야 한다.
3. 개인정보파일을 파기하는 경우, 개인정보보호위원회에 등록된 개인정보파일 목록 등도 함께 삭제될 수 있도록 해야 한다.

지표 해설

- 개인정보 보호책임자는 개인정보파일 파기 시행 후 파기 결과를 확인하고 개인정보파일 파기 관리대장을 작성하여야 한다.(표준지침 제55조)
- 개인정보를 수집했던 목적이 달성되어 보존 필요성이 없어졌는데도 이를 계속해서 보유할 경우 개인정보의 유출과 오용 가능성이 높아지므로 더 이상 개인정보가 불필요하게 된 때에는 이를 파기시킴으로써 개인정보를 안전하게 보호하려는 것이다.
- 개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기해야 한다. "개인정보가 불필요하게 되었을 때"란 개인정보의 처리목적이 달성되었거나, 해당 서비스의 폐지, 사업의 종료 된 경우 등이 포함된다. 따라서 개인정보처리자는 처리목적이 달성되거나, 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한, 5일 이내에 개인정보를 파기하여야 한다(표준지침 제10조제1항). 개인정보의 보존 필요성이 있는지 여부는 객관적으로 판단하여야 하며 자의적으로 해석해서는 안 된다.
- 개인정보처리자가 개인정보 보유기간을 고지하고 동의 받는 경우 그 보유기간을 정할 때에는 그 보유목적이 명백히 영구히 보유하여야 하는 경우에는 영구, 그렇지 않은 경우 필요 최소한으로 정해야 한다. 이 경우 입증책임은 개인정보처리자가 부담한다.

- 개인정보처리자는 개인정보의 파기에 관한 사항을 기록하고 관리하여야 한다. 보유목적을 달성한 개인정보의 파기는 법적 의무사항이며 위반시 벌칙이 부과되는 사항이므로 파기는 반드시 개인정보 보호책임자의 책임하에 수행되어야 하며, 개인정보 보호책임자는 파기 결과를 확인하여야 한다.(표준지침 제10조 제3항부터 제5항)
- 개인정보처리자는 '다른 법령에 따라 보존해야 하는 경우'에는 예외적으로 개인정보를 파기하지 않아도 된다. 개인정보처리자가 개인정보를 파기하지 않고 보존하려고 하는 경우에는 그 법적 근거를 명확히 해야 한다. 채권소멸기간까지 개인정보를 보존할 수 있다고 하여 이미 요금정산이 끝난 소비자의 개인정보까지 보존하여서는 안 된다. 신용카드 이용고객의 신용관리를 이유로 회원의 동의 없이 탈퇴회원의 개인정보를 일정기간 보존하는 것도 파기의무 위반이다. 다른 법령에서 보존기간으로 정한 기간이 만료한 경우에는 지체 없이 파기하여야 한다.
- 개인정보파일을 파기할 때에는 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기하여야 한다.(단, 파기방법의 적정성 및 안전성에 대해서는 지표 4.7.1에서 점검)

■ 표준 개인정보 보호지침 [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			

■ 표준 개인정보 보호지침 [별지 제5호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
3.5.3	개인정보파일을 파기하는 경우 파기 결과 등을 '개인정보파일 파기 관리대장'에 기록·관리 하도록 계획하고 있습니까?	○			
평가근거 및 의견	● △△△ 기관은 '○○○ 발송 정보', '○○○ 위원 현황' 등 5건의 개인정보 파기 사실이 있어 4건에 관해서는 '개인정보 파기 대장'에 기록하였으나 'XXX 현황'에 대한 파기 사실은 누락되어 있음.				

개인정보 파기 대장

개인정보파일 파기 대장

2013.05.31

No.	부서명	개인정보파일명	근거	목적	주요항목	보유기간	대상인원	파기일 및 파기사유
1	○○○실	○○○ 발송 대상	○○○법 제4조	○○○ 배포	성명, 이메일, 휴대폰 번호	3년	10,000	파기 (○○○팀-1505, 2013.5.21)
2	○○○실	○○○ 위원 정보	○○○ 처리 규칙	○○○ 위촉	성명, 휴대폰번호, 주소, 전화번호, 주민번호, 소속	5년	150	파기 (○○○○지원-1108, 2013.5.23)
3	○○○실	○○○ 심사원 목록	○○○처리에 관한 규칙	○○○ 위촉	성명, 핸드폰번호, 주소, 전화번호, 소속	5년	120	파기 (○○○원-1108, 2013.5.23)
4	○○○○실	○○○운영위원 목록	○○○ 운영 지침	○○○XX 위촉	성명, 이메일, 휴대폰번호, 주민번호, 주소, 전화번호, 소속	3년	20	파기 (○○○원-1108, 2013.5.23)

관련법령 및 문서

관련 법령 · 지침

【표준 개인정보 보호지침】

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 등록사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제21조

4. 대상시스템의 기술적 보호조치

1 접근권한 관리

세부분야	개인정보 수집의 적합성				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.1	● **개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보처리시스템에서 응용프로그램, 서버, DBMS 중 일부에서 한 개의 ID를 발급하여 여러 명이 사용하는 경우				
평가근거 및 의견	● ○○기관은 내부 관리계획의 기술적 안전성 확보조치 사항에 "한 명의 직원에게 한 개의 ID발급을 원칙으로 한다"라고 명시되어 있으나, 서버, DBMS는 개별계정이 부여되어 있으나, 응용프로그램에서 ○○팀 담당자는 본인의 ID를 동료직원과 공유하여 업무를 처리하고 있음				

주요 점검 사항

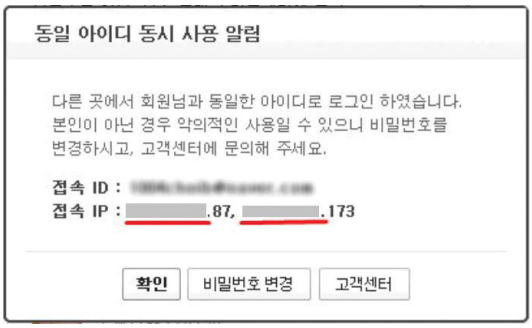
1. 개인정보처리시스템에 접속할 수 있도록 사용자 계정을 발급하는 경우, 책임추적성이 확보될 수 있도록 개인정보취급자별로 고유한 사용자 계정을 발급하여야 한다.
   ※ 개인정보처리시스템과 관련된 응용프로그램, 서버, DBMS 계정 포함
2. 개인정보취급자의 사용자 계정은 다른 개인정보취급자와 공유되지 않도록 해야 한다.

지표 해설

- 개인정보처리자는 개인정보처리시스템에 접근하는 개인정보취급자 별로 한 개의 고유 ID를 부여하고 다른 개인정보취급자와 공유되지 않도록 관리하여야 한다.
  - 개인정보가 처리되는 응용프로그램, DBMS, 서버 등의 접근계정은 1인 1계정을 발급하고, 발급된 계정은 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
- 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 ID를 공유하지 않도록 하여야 하며 1인 1계정 발급을 통해 개인정보 처리내역에 대한 책임 추적성 (Accountability)을 확보하여야 한다.
- 한 명의 개인정보취급자가 여러 업무를 수행해야 하는 경우, 해당 개인정보취급자에게 각 업무별로 사용자 계정을 발급할 수 있다(예 : 개인정보취급자 1명이 서로 권한이 다른 조회, 삭제 등 2개의 업무 수행 시에 조회 업무용과 삭제 업무용으로 구분하여 2개의 사용자 계정 발급 가능함). 이는 이 경우에도 하나의 ID당 한명의 개인정보취급자가 연결됨으로 인하여 책임추적성이 확보될 수 있기 때문이다.
- 시스템 설치 후 제조사 또는 판매사의 기본 계정 및 시험 계정 등은 제거 또는 추측이 어려운 계정으로 변경하여 비인가자에게 노출되거나 공유하여 사용되지 않도록 하는 것이 권장된다.

- 시스템 계정 등 정보시스템 환경 상 혹은 업무상 불가피하게 사용자 계정을 공유하여 사용할 경우 사유와 타당성을 검토하여 책임자의 승인을 받도록 하는 것이 바람직하며 책임추적성을 보장할 추가적인 통제 방안을 적용하여야 한다.

평가 예시

<table>
<tr><th>구 분</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>4.1.1</td><td>개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하도록 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가근거 및 의견</td><td colspan="5">
● ○○기관은 내부 관리계획의 기술적 안전성 확보조치 사항에 “한 명의 직원에게 한 개의 ID발급을 원칙으로 한다.”라고 명시되어 있으나, 서버, DBMS 계정은 문제가 없으나 ○○홈페이지 관리자 ID계정 한 개를 A직원과 B직원이 함께 사용하여 업무를 처리하고 있음.
<table>
<tr><th>구분</th><th>분석내용</th></tr>
<tr><td>응용프로그램</td><td>관리자 ID계정 한 개로 A직원, B직원이 함께 사용하고 있음</td></tr>
<tr><td>서버</td><td>서버관리자 1명이 지정되어 있고, 한 개의 ID계정으로 사용</td></tr>
<tr><td>DBMS</td><td>DB관리자 1명이 지정되어 있고, 한 개의 ID계정으로 사용</td></tr>
</table>
<table>
<tr><td>ID 동시접속 알림창</td><td>


</td></tr>
</table>
</td></tr>
</table>

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제23조(민감정보의 처리 제한) 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.

제24조(고유식별정보의 처리 제한) 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.

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.

【개인정보 보호법 시행령】

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.2	● **개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 비밀번호 설정 시 최소길이(조합도 포함), 동일한 비밀번호 사용제한, 추측 가능한 문자열 포함 제한 등 조합규칙 중 일부만 적용하는 경우				
평가근거 및 의견	● ○○기관의 개인정보취급자의 ○○관리시스템 접속 시 계정 비밀번호 설정은 영문, 숫자, 특수문자를 조합하여 8자리 이상의 길이 제한을 하고 있으나, 일련번호, 동일한 비밀번호 사용제한, 일련번호 등의 제한 여부는 적용하지 않음				

주요 점검 사항

1. 개인정보취급자가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
   ① 최소 길이 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우 8자리 이상, 2종류 이상으로 구성한 경우 10자리 이상
   ② 변경 주기 : 최소 반기 1회 이상
   ③ 기타 : 추측하기 쉬운 문자·단어 제한(일련번호, 전화번호, 잘 알려진 단어 등), 동일한 비밀번호 재사용 제한 등
2. 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립하여 적용해야 한다.
   ※ 단, 정보주체의 편의성 등을 고려하여 자율적으로 적절한 수준을 설정하여 이행
3. 대상기관의 내부 규정(보안지침 등)에 비밀번호 작성규칙이 별도로 명시되어 있다면, 해당 규정도 준수할 수 있도록 해야 한다.

지표 해설

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용하여야 한다. 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성 하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다.

- 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있다. 안전한 비밀번호란 제3자가 쉽게 추측할 수 없으며 비밀번호 해킹 등을 통해서도 비밀번호를 얻어낼 수 없거나 얻어내는데 많은 시간이 요구되는 것을 의미한다. 따라서 개인정보취급자나 정보주체가 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 개인정보처리시스템에 적용하여야 한다.
  - 비밀번호 설정·변경 시 입력 값의 자리수와 조합을 체크하여 안전한 비밀번호 작성규칙에 위배되는 경우, 법 위반임을 알리고 작성규칙을 준수토록 하여야 한다.

- 비밀번호의 설정·변경 후 6개월 경과 시 비밀번호 변경 화면을 띄워 비밀번호를 변경할 수 있는 기능을 제공하여야 한다.

- 비밀번호는 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, 변경 주기는 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.

- 비밀번호 작성규칙을 수립한 경우 개인정보취급자 또는 정보주체가 비밀번호를 사용하고자 할 경우 일정 수준 이하의 비밀번호는 설정되지 못하도록 하거나, 주기적으로 패스워드를 변경하지 않을 경우, 시스템 내 사용을 제한하도록 시스템을 통해 자동화 기능을 구현할 수 있다.

- 개인정보취급자와 달리 정보주체의 비밀번호는 정보주체의 편의성 등을 고려하여 개인정보처리자가 자율적으로 적절한 수준을 설정하는 것이 가능하다. 다만 이 경우에도 정보주체의 편의성만을 고려하여 비밀번호 작성규칙을 전혀 적용하지 않는 것은 바람직하지 않으며, 편의성과 보안성의 균형을 잘 고려하여 최소한의 비밀번호 작성규칙은 적용될 수 있도록 기준을 마련하고 적용할 필요가 있다.

- 시스템에서 초기에 설정된 디폴트 패스워드는 변경하여 사용하고, 예제 등으로 제시되고 있는 널리 알려진 패스워드는 사용을 금지하여야 한다.

- 대상 기관이 적용받는 타 법률, 국가정보보안 기본지침 등 상위 기관의 정보보안 지침, 대상 기관 내부의 정보보안 지침 등에서 비밀번호 작성규칙이 명시되어 있다면 해당 지침도 동시에 준수할 수 있도록 비밀번호 작성규칙을 적용할 필요가 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.2	개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?		○		

평가근거 및 의견

- ○○기관의 개인정보취급자의 ○○관리시스템 접속 시 계정 비밀번호 설정은 영문, 숫자, 특수문자를 조합하여 6~20 자리, 아이디와 3자리 이상의 중복여부 등에 대한 조합규칙을 적용하고 있으나, 최소한의 길이가 8자리 이하로 비밀번호 조합규칙의 조건에 미흡하며, 동일한 비밀번호 사용제한 등이 적용되어 있지 않음.

구분	분석내용
응용프로그램	개인정보취급자 비밀번호는 6~20자로 되어 있어 적정하지 않음
서버	서버관리자 비밀번호는 3개 조합으로 9자리로 적용되어 있음
DBMS	DB관리자 비밀번호는 3개 조합으로 9자리로 적용되어 있음

ID 동시접속 알림창

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.3	● **정보주체가 비밀번호 변경 등 중요 정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용되도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 비밀번호 등 중요 정보 조회·변경 시 비밀번호 재확인 등의 추가 인증절차가 적용되어 있지 않는 경우				
평가근거 및 의견	● ○○기관 인터넷 홈페이지에서 비밀번호 변경 시 기존 비밀번호 재확인 없이 신규 비밀번호가 입력하면 변경이 가능하도록 설정되어 있음				

주요 점검 사항

1. 정보주체가 인터넷 홈페이지 등을 통해 중요한 정보 또는 화면에 접근하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공동인증서 등 본인임을 확인할 수 있는 추가적인 인증 절차가 적용되어야 한다.
   ※ 회원정보 조회·변경(민감한 정보 포함 시), 아이디 찾기, 비밀번호 찾기, 증명서 발급신청 등
   ※ "중요 정보"의 기준은 대상 기관 및 시스템의 개인정보 영향도 기준 등을 참고하여 결정

지표 해설

- 정보주체가 인터넷 홈페이지에 로그인한 채로 자리를 비운 상태에서 제3자가 해당 PC에 접근하거나 해킹으로 인하여 로그인한 사용자의 세션 값이 탈취당하는 경우, 정보주체의 중요 개인정보가 비인가자에게 노출되거나 불법적으로 변경될 위험성이 존재한다.
- 이러한 위협에 대응하기 위해서는 정보주체가 인터넷 홈페이지 등에 정상적으로 로그인된 상태라 하더라도 고유식별정보(주민등록번호, 운전면허번호, 여권번호, 외국인 등록번호), 민감정보(병력 등), 금융정보(계좌번호, 카드번호 등), 비밀번호 등 중요한 정보를 조회하거나 변경하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공동인증서 등의 본인임을 확인할 수 있는 추가적인 인증 절차를 적용하는 것이 권고된다. 다만 주민등록번호, 계좌번호 등 중요한 개인정보에 개인정보 표시제한 조치(마스킹 등)를 적용하여 원본 정보 확인이 어려운 경우에는 추가적인 본인 인증이 필요하지 않을 수 있다.
- 또한, 아이디 찾기, 비밀번호 찾기 등 로그인 없이도 접근이 가능한 화면에서 본인 여부를 확인하는 절차상에 취약점이 존재할 경우에도 이를 악용하여 계정을 도용하거나 회원 정보를 유출하는 등의 불법적인 행위가 발생할 가능성이 존재한다.
- 이에 대응하기 위해서는 아래와 같이 사전에 정보주체가 입력한 정보(이메일, 휴대폰 등)를 이용하거나, 아이핀 등 별도의 본인확인 수단을 적용하는 등의 안전한 본인 확인 절차를 가져갈 필요가 있다.

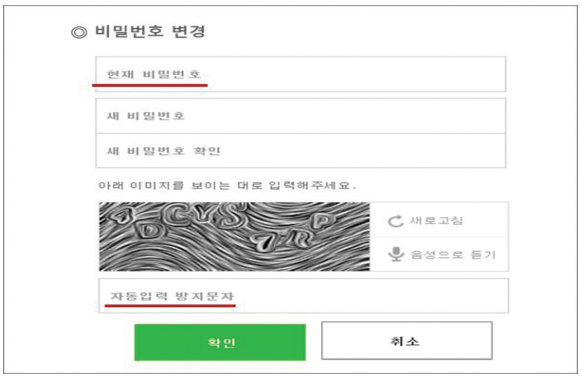
아이디 찾기 (예시)	
1. 회원정보 이용	· 이름 + 생년월일 + 휴대번호 입력 → 아이디 일부만 표시
	· 이름 + 생년월일 + 이메일 입력 → 아이디 일부만 표시
	· 이름 + 휴대번호 입력 → SMS인증번호 입력 → 아이디 표시
	· 이름 + 이메일 입력 → 인증코드(이메일 발송) 입력 → 아이디 표시
	· 이름 + 이메일 입력 → 이메일 발송(아이디)
2. 본인확인수단 이용	· 본인 명의 휴대전화 인증
	· 아이핀 인증

비밀번호 찾기 (예시)
- 아이디 + 성명 + 가입 시 등록한 휴대번호 : SMS로 임시 비밀번호 발급 - 아이디 + 성명 + 가입 시 등록한 이메일주소 : 이메일주소로 임시 비밀번호 발급 - 아이디 + 성명 + 가입 시 등록한 힌트 : 임시 비밀번호 표시 - 아이디 + 아이핀 인증 : 임시 비밀번호 표시 - 아이디 + 휴대폰 본인 인증 : 임시 비밀번호 표시 ※ 임시 비밀번호 발급 시에는 최초 로그인 시 비밀번호를 변경하도록 설정 필요

- 본 항목은 개인정보의 안전성 확보를 위한 권장 사항으로서 대상 시스템의 특성이나 위험성 등을 고려하여 적용 여부 및 수준을 결정하여 시행할 필요가 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.3	정보주체가 비밀번호 변경 등 중요정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용되도록 계획하고 있습니까?	○			
평가근거 및 의견	● 인터넷 홈페이지 “비밀번호 변경” 시 기존 비밀번호 확인, 자동입력 방지문자가 적용되어 있으며, “비밀번호 찾기” 시 휴대폰, 이메일, 힌트, 아이핀 인증을 통해 본인여부를 확인하는 절차를 가져가고 있음				

비밀번호 변경화면 (기존 비밀번호 확인)	
비밀번호 찾기 화면 (휴대폰, 이메일, 힌트, 아이핀 인증)	

관련법령 및 문서

관련 법령 · 지침

● 본 항목은 ‘개인정보 안전조치 의무’를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.4	● **대량의 개인정보 또는 중요한 개인정보를 처리하는 개인정보취급자 및 관리자는 강화된 인증방식이 적용되도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 개인정보처리시스템에 접근 시 공인인증서, OTP 등의 안전한 인증방식으로 설계하고 있는 경우				
평가근거 및 의견	● 관리자페이지는 아이디, 비빌번호 방식으로 인증을 하지 않고, 공동인증서 방식으로 인증처리를 하고 있음				

주요 점검 사항

1. 대량의 개인정보 또는 중요한 개인정보를 처리하는 개인정보취급자 및 관리자는 권한 도용 등을 방지하기 위하여 강화된 인증방식이 적용되어야 한다.

※ 소유기반 인증(인증서, OTP, 보안토큰 등), 생체기반 인증(지문, 홍채, 정맥 등), 위치 기반(IP 주소 지정 등) 등

※ "중요 정보"의 기준은 대상 기관 및 시스템의 개인정보 영향도 기준 등을 참고하여 결정

지표 해설

- 대량의 개인정보 또는 중요한 정보를 취급하는 자가 개인정보처리시스템 접속 시 단순히 아이디와 비밀번호만을 이용할 경우, 키로깅(Key logging) 등에 의해 아이디와 비밀번호만 유출되어도 개인정보처리시스템이 위험에 노출되게 된다. 이러한 위험성을 감소시키기 위해 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 인증서 등을 활용한 추가적인 인증 수단의 적용이 필요하다.
- 강화된 인증에는 다양한 방식이 적용될 수 있으므로 대상 시스템의 특성 및 위험도 등을 고려하여 적용 대상 및 인증 방식을 선택할 필요가 있다.

강화된 인증 방식 예시		
구 분	인증 방식	비 고
소유 기반	인증서(PKI)	- 공동인증서(NPKI) - GPKI인증서행정전자서명 인증서), EPKI인증서 - 사설인증서 : 자체 CA서버 구축 등
	OTP	- One Time Password - 무작위로 생성되는 일회용 패스워드를 이용하는 사용자 인증방식 - OTP토큰 방식, 모바일OTP 방식 등
	스마트폰	- SMS 인증 등
	기타	- 스마트카드 방식 - 물리적 보안토큰 방식 등
생체 기반	신체적 특징	- 지문 : 가장 보편적으로 사용하는 방식 - 홍채, 안면, 정맥 등
	행동적 특징	- 서명, 키스트로크, 음성인식 등
기타 방식	IP 주소	- 특정 IP주소에서만 해당 아이디로 접속할 수 있도록 제한하는 방식
	MAC 주소	- 단말기의 MAC주소를 기반으로 등록된 단말기에서만 접속할 수 있도록 제한하는 방식
	기기 일련번호	- 특정 PC 또는 특정 디바이스(스마트폰 등)에서만 접속할 수 있도록 제한하는 방식
	기타	- 로그인 시 매번 다른 비밀번호를 생성·발급하여 사용 (패스워드 관리 시스템 도입 등)

- 인증서 방식의 경우 PC에 인증서를 저장할 경우 악성코드 감염 등에 따라 인증서가 외부에 유출될 수 있으므로 가급적 별도의 보안매체에 보관하는 것을 권장한다.

【용어설명】

※ GPKI(Government Public Key Infrastructure) : 행정전자서명 인증체계

※ EPKI(Education Public Key Infrastructure) : 교육부 전자서명 인증체계

※ NPKI(National Public Key Infrastructure) : 국가에서 인증한 기관에서 발행하는 민간 인증체계

평가 예시

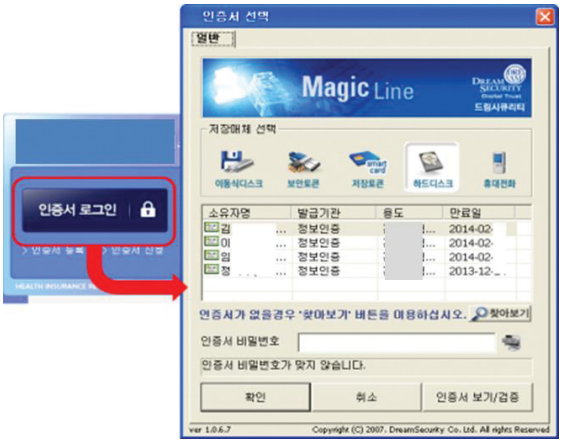
구 분	질의문	이행	부분이행	미이행	해당없음
4.1.4	대량의 개인정보 또는 중요한 개인정보를 처리하는 개인정보취급자 및 관리자는 강화된 인증방식이 적용되도록 계획하고 있습니까?	○			

평가근거 및 의견

- 관리자 페이지는 아이디, 비밀번호 방식으로 인증을 하지 않고, 공동인증서 방식으로 인증처리를 하고 있으며, 서버 및 DBMS는 관리용단말기에서만 접속되도록 접근통제가 적용되어 있음

구분	분석내용
응용프로그램	관리자 인증은 공동인증서 방식적용
서버	서버관리자 지정된 관리자 단말기에서만 접속되도록 통제
DBMS	DB접근제어 솔루션이 구축되어 지정된 DB관리자만 접근하도록 통제

인증서를 통한 인증



관련법령 및 문서

관련 법령 · 지침

- 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.5	● **개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하고 있습니까?**		○		
평가 예시	● 부분이행 : 일정 횟수 이상 비밀번호 입력 오류에 따른 경고 메시지는 있으나 차단되도록 설계되어 있지 않음				
평가근거 및 의견	● 로그인 화면에 "비밀번호 3회 입력 오류 시 로그인 접속이 제한됩니다"라는 메시지는 기재되어 있으나 실질적으로 차단되도록 설계되어 있지 않음				

주요 점검 사항

1. 개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정 정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 보호조치를 하여야 한다.

지표 해설

- 개인정보처리시스템에 비정상적인 접근에 대한 방지 대책이 없다면 개인정보취급자 계정 도용 등에 따라 정보주체의 개인정보가 유출, 변조, 훼손될 위험이 존재하므로 이에 대한 대책 마련이 필요하다.
- 일정 횟수 이상의 비밀번호 입력오류가 발생할 경우 경고메시지와 함께 더 이상의 인증시도를 막을 수 있도록 보호조치를 취하여야 한다.
  - 로그인 화면에서 연속적으로 일정 횟수(예를 들어, 5회) 이상 비밀번호 오류 입력 시 시스템 접속을 차단하도록 한다.
  - 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에도 반드시 정당한 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요하다.
- 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(공동인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인하는 조치를 취하는 것도 가능하다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.5	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 로그인 실패횟수 제한, 최대 접속시간 제한, 동시 접속 제한, 관리자 로그인 알림 등 보호대책이 적용되도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○기관 '시스템관리 업무 매뉴얼 패스워드 작성 규칙' 내에는 '모든 사용자의 비밀번호 입력 제한은 3회 이하로 하고, 실패 시 계정은 잠기며 관리자에 의해 비밀번호를 재설정한 후 사용할 수 있다'고 기재되어 있으나, 실질적으로 차단되도록 설계되어 있지 않음				

시스템관리 업무 매뉴얼 패스워드 작성 규칙	나. 패스워드 관리 (1) 패스워드 관리 정책 ○ 사용자의 패스워드는 주기적으로 변경해야 한다.(90일 이내) ○ 모든 사용자의 패스워드는 문자/숫자/특수문자를 포함하여 8자리 이상으로 한다. ○ 최근 사용한 5번 이내의 패스워드는 재사용 할 수 없다. ○ 모든 사용자의 패스워드 입력 제한은 3회 이하로 하고, 실패 시 계정은 잠기며, 관리자에 의해 패스워드를 재 설정한 후 사용할 수 있다. ○ 기존 사용자가 이/퇴직, 업무변경 등의 사유로 계정을 인수받는 인수자는 즉시 기존 패스워드를 변경해야 한다. ○ 패스워드 만료일 이전 10일부터 변경알림을 사용자 접속 시 알려야 한다.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.6	● **개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 계획하고 있습니까?**		○		
평가 예시	● 이행 : 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 기능 설계 및 구현된 경우				
평가근거 및 의견	● ○○대학교 개인정보취급자가 업무를 처리하는 학사행정시스템, 포털사이트에 세션타임 기능이 적용되도록 설계되어 구현되어 있음				

주요 점검 사항

1. 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.
   ① 개인정보취급자가 일정시간 이상 업무처리를 하지 않은 경우 개인정보처리시스템에 대한 접속이 차단되도록 기능 설계 및 구현여부 확인
   ② 다시 접속하고자 할 때에도 최초의 로그인과 동일한 방법으로 접속하도록 해야 함

지표 해설

- 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않은 경우 자동으로 접속이 차단되도록 하여야 한다. 이는 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미하며, 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않는다.
- 이러한 접속차단 조치는 개인정보처리시스템과 연결이 완전히 차단되어 정보의 송·수신이 불가능한 상태가 되어야 하며, 접속차단 조치 이후에 다시 접속하고자 할 때에는 최초의 로그인 방법과 동일한 방법으로 접속하도록 하여야 한다.
- 접속차단을 적용하기 위한 시간 기준은 개인정보를 처리하는 방법 및 환경, 보안위험 요인, 업무특성(DB 운영관리, 시스템 모니터링, 유지보수 등)을 고려하여 필요 최소한의 시간으로 설정할 필요가 있다.
- 본 조치는 개인정보처리시스템을 대상으로 적용해야 하므로, 응용프로그램 외에 서버, DBMS도 평가범위에 포함된다면 해당 영역에 대해서도 일정시간 업무처리를 하지 않은 경우에는 자동으로 접속이 차단되도록 조치할 필요가 있다.

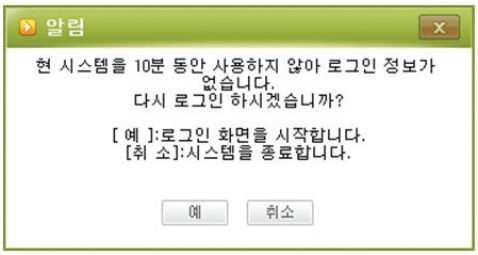
평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.6	개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 계획하고 있습니까?	○			

평가근거 및 의견

- ○○대학교 개인정보취급자가 업무를 처리하는 학사행정시스템, 포털사이트에 세션타임 아웃 기능이 적용되도록 설계되어 구현되어 있음
- 각각 설계되어 있는 세션타임 아웃 기능은 아래와 같음

구분	분석내용
학사행정시스템	세션타임 아웃 기능 : 1시간으로 구현됨
포털사이트	세션타임 아웃 기능 : 10분 으로 구현됨

학사행정시스템 로그인 세션 잠김 화면	
포털사이트 로그인 세션 잠김 화면	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(접근통제) ⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.7	● **개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 장기 미접속시 계정 잠금, 동시 접속 제한, 관리자 로그인 알림 등 보호 대책이 적용되도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보처리시스템 보호대책을 위해 동시 접속 제한 기능 등 일부만 설계되어 있는 경우				
평가근거 및 의견	● ○○시스템에 대한 보호조치를 위해 관리자 로그인 알림 기능만 설계되어 구현되어 있고, 장기 미접속시 계정 잠금 기능, 동시 접속 제한 기능에 대한 설계 및 구현이 되어 있지 않음				

주요 점검 사항

1. 개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위한 보호대책이 적용되어야 한다.
   ① 업무 시간 외 접속 가능 시간 제한
   ② 일정기간 미접속 시 계정 잠금
   ③ 동일 계정에 대한 동시 접속 제한
   ④ 관리자 등 특수권한 로그인 시 알림 기능
   ⑤ 기타 비정상적인 접근을 탐지 또는 방지할 수 있는 보호조치

지표 해설

- 개인정보처리시스템에 비정상적인 접근에 대한 방지 대책이 없다면 개인정보취급자 계정 도용 등에 따라 정보주체의 개인정보가 유출, 변조, 훼손될 위험이 존재하므로 이에 대한 대책 마련이 필요하다.
- 이러한 비정상적인 접근을 탐지 또는 차단할 수 있는 방법에는 업무 시간 외 접속 가능 시간 제한, 동시 접속 제한, 로그인 알림 기능, 일정기간 미접속 시 계정 잠금 등 다양한 방법이 있으며, 대상 개인정보처리시스템이 보유하고 있는 개인정보의 민감도, 대상 시스템의 특성, 개인정보 침해 위험도 등을 고려하여 적용 방식 및 수준을 결정하여 시행할 필요가 있다.
- 중요 개인정보처리시스템의 경우 업무시간 이외에는 사용을 통제하고, 사용 필요시 사유 등과 함께 관리하여 업무시간 외에 발생하는 개인정보 무단 조회 등에 대비하는 것을 권장한다.
  · 업무시간은 일반적으로 09:00~18:00 이지만 업무의 처리 및 특성을 고려하여 개인정보처리시스템 설계 시 업무시간을 정의할 것을 권장한다.

· 업무시간 이외에 접속을 차단하지 아니하고 사유 입력 등을 통해 관리하도록 설계를 하는 경우는 해당 사유에 대한 로그정보가 기록관리 되도록 하는 것이 바람직하다. 로그정보는 누가, 언제, 사용목적 등에 대한 정보를 기록하도록 할 것을 권장한다.

· 대상 시스템 특성 상 24시간 운영 등의 이유로 업무시간을 정의할 수 없다면 본 조치를 적용하지 아니할 수 있다.

- 개인정보처리시스템의 계정 노출 등에 따라 다수의 PC에서 개인정보처리시스템 접근 시 정상적인 사용자가 이를 인지할 수 있도록 중복 로그인을 차단하도록 설계하는 것이 바람직하다. 중복로그인이 발생하는 경우 차단사실과 함께 중복로그인 위치의 간단한 정보도 함께 알려주는 것을 권장한다.

- 특히, 다른 개인정보취급자의 권한을 설정하거나 개인정보처리시스템의 주요 설정을 변경할 수 있는 관리자 계정으로 로그인하는 경우 관리자에게 자동 고지함으로써 관리자 계정의 노출 및 오용 여부를 쉽게 파악할 수 있으며, 이 경우 SMS, 이메일 등의 방법 활용을 권장한다.

- 특정기간(1개월 등) 이상 개인정보처리시스템에 로그인하지 않은 계정은 미사용 계정으로 분류하여 접근을 차단한다. 특정기간 이후에도 내부절차에 따라 계정사용 요청을 할 수 있도록 마련하고, 특정기간 이상 로그인이 없는 계정은 휴면계정으로 처리하여 접근차단을 권장한다.

- 개인정보처리시스템의 중복 로그인을 차단할 수 있는 기술적 방법으로는 로그인을 위한 인증정보를 아이디 및 비밀번호와 함께 IP 또는 Mac주소 정보까지 포함할 경우, 지정된 PC에서만 로그인을 할 수 있으므로 중복 로그인을 차단할 수 있다. 일반적으로, IP 또는 Mac주소까지 인증정보에 포함하는 경우는 관리자 계정(admin) 로그인 시 활용할 것을 권장한다.

평가 예시

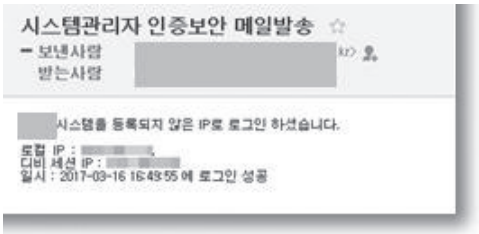
구 분	질의문	이행	부분이행	미이행	해당없음
4.1.7	개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 장기 미접속시 계정 잠금, 동시 접속 제한, 관리자 로그인 알림 등 보호 대책이 적용되도록 계획하고 있습니까?		○		

평가근거 및 의견

- ○○시스템에 대한 보호조치를 위해 관리자 로그인 알림 기능은 설계에 반영되어 있으나, 장기 미접속시 계정 잠금, 동시 접속 제한 기능에 대해서는 설계에 반영되어 있지 않음

보호조치	OO시스템
장기 미 접속 시 계정잠금	해당 기능이 설계에 반영되어 있지 않음
동시 접속 제한	해당 기능이 설계에 반영되어 있지 않음
관리자 로그인 알림	설계에 반영되어, 현재 테스트로 구현되어 있음

관리자 로그인 알림 기능 (테스트 결과)



관련 문서

- 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

세부분야	권한 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.8	● **개인정보취급자가 변경될 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보취급자 변경 시 임직원의 경우 개인정보처리시스템 접근권한을 변경하거나 제거되도록 설계하고 있으나 임시직 및 시간제근무자에 대해서는 적용이 누락된 경우				
평가근거 및 의견	● 임직원은 인사시스템과 개인정보처리시스템간의 인사정보 연동을 통하여 개인정보취급자 발령, 퇴직 등의 변경사항이 발생하면 지체없이 개인정보처리시스템 권한이 변경, 삭제되도록 되어 있으나, 임시직 및 시간제근무자는 자동으로 연계되어 있지 않아 개인정보처리시스템 관리자에게 제때 통보를 하지 못해 접근권한 변경 또는 말소 작업이 즉시 이루어지지 않고 있음				

주요 점검 사항

1. 전보, 퇴직 등 인사 이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.
   ① 관리적으로 조치하는 경우에도 누락 없이 변경 또는 말소 될 수 있도록 내부 관리계획 등에 반영하여 이행하도록 절차 마련
   ② 협력업체 인원 등 정직원이 아닌 경우에도 누락 없이 반영될 수 있도록 주의

지표 해설

- 개인정보취급자가 변경 될 경우 개인정보처리시스템에 관한 접근권한을 변경 또는 말소하여 업무가 바뀐 개인정보취급자가 개인정보처리시스템의 개인정보를 이용하지 못하게 하여야 한다.
- 조직 내의 임직원 전보 또는 퇴직 등 인사이동을 통해 사용자 계정의 변경·삭제가 필요한 경우에는 공식적인 사용자 계정 관리절차에 따라 통제될 수 있도록 한다.
  - 내부 인력의 전보 또는 퇴직 시 해당 인력의 계정을 지체 없이 변경 또는 말소하도록 내부 관리계획, 개인정보 보호 지침 등에 반영하여 이행하도록 한다.
  - 임직원의 퇴직 시 계정 삭제를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용 계정의 삭제항목을 반영하여, 계정의 삭제 여부에 대해 확인을 받을 수 있다.
- 외부 인력의 업무 변동 및 계약 종료 등으로 인한 사용자 계정의 변경삭제가 필요한 경우에는 조직 내의 외부 인력 담당자가 해당 계정의 변경 및 삭제를 처리하며, 외부 인력 업무 변동 및 계약 종료 시 계정을 즉시 변경 또는 말소하도록 공식적인 관리절차를 수립하여 통제될 수 있도록 권장한다.

- 응용프로그램, DB, 서버 등 개인정보처리시스템의 접근권한은 인사시스템과 연동하여, 조직 내의 임직원 전보 또는 퇴직 등 인사이동 내역이 인사시스템에 반영될 경우, 자동으로 개인정보처리시스템의 접근권한을 변경 및 삭제할 수 있도록 시스템화할 것을 권장한다.
- 또한, 인사시스템 연계 등을 통해 자동화 하더라도 운영 과정에서 임시로 등록되는 계정들이 존재할 수 있다. 이러한 계정들을 수작업으로 검토하여 조치하는 것은 현실적으로 어려움이 있을 수 있으므로, 관리적인 절차 마련과 함께 개인정보처리시스템에서 임시 등록 계정, 일정 기간 미사용 계정, 특수권한이 부여된 계정 등을 쉽게 검색하여 조치할 수 있도록 응용프로그램의 기능으로 구현하는 것을 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.8	개인정보취급자가 변경될 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○시스템은 계정 변경 및 삭제할 수 있도록 설계되어 있으나, 개인정보취급자 발령, 퇴직 등의 변경사항이 발생하면 인사담당자는 인사업무를 처리 하고 문서 또는 구두로 개인정보처리시스템 관리자에 통보하여 개인정보취급자에 대한 접근권한 변경 또는 말소 처리하도록 하고 있으나, 인사담당자가 인사업무처리 즉시 알려주지 않아 일정기간이 지났음에도 개인정보취급자에 대한 접근권한 변경 또는 말소가 되지 않고 있음				

OO시스템 계정 변경 및 삭제 설계	`GnfdAuthSmeBtchVO gnfdAuthSmeBtchVo = new GnfdAuthSmeBtchVO();`
	`// Database를 처리하는 reader/writer의 경우 수행할 query를 불러온다.`
	`// 발령정보에 따른 권한회수 대상자를 조회하는 SQL 로딩`
	`reader1.loadSQL("selectGnfdUsr");`
	`// 대상자에 한해서 권한회수를 하기 위한 SQL 로딩(TBCOA006 삭제, TBCOA007 변경)`
	`writer1.loadSQL("deleteGnfdUsrAuth");`
	`writer2.loadSQL("updateGnfdUsrAuthHist");`

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

세부분야	권한 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.9	● **개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 기록하도록 계획하고 있습니까?**		○		
평가 예시	● 부분 이행 : 접근권한 기록을 저장하고 있으나 보관 기간이 3년 미만이거나, 등록일자 등 일부 정보가 미기록 되어 있거나, 일부 사용자에 대하여 접근권한 기록이 누락되는 경우가 존재하는 경우 등				
평가근거 및 의견	● ○○시스템의 개인정보취급자 접근권한을 발급·변경·삭제한 기록이 저장되어 보관되고 있으나, 보관 기간이 최소 요건인 3년보다 적은 2년간만 보관되고 있음				

주요 점검 사항

1. 개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역은 책임추적성을 확보할 수 있도록 관련 사항이 모두 포함되어 기록되어야 한다.
   ① 대상자 정보(식별자 등)
   ② 접근권한 부여자 정보(담당자, 승인자 등)
   ③ 접근권한 정보(일시, 권한명, 사유 등)
   ④ 기타 접근권한 검토를 위해 필요한 정보(특이사항 등)
2. 접근권한 기록은 최소 3년간 보관하여야 한다.
3. 접근권한의 적정성을 상세히 검토할 수 있도록 접근권한 기록 검토방안을 마련하여야 한다.

지표 해설

- 4.1.8【지표 해설】 참조
- 「개인정보의 안전성 확보조치 기준」 고시에 따르면 개인정보처리시스템에서 개인정보 취급자의 권한을 부여, 변경, 말소한 기록은 최소 3년간 보관하도록 명시하고 있다. 참고적으로 정보통신서비스제공자일 경우에는 「개인정보의 기술적·관리적 보호조치 기준」에 따라 최소 5년간 보관하여야 한다.
- 개인정보처리시스템의 접근권한 기록은 사후에 문제 발생 시 권한 발급 이력을 정확하게 파악할 수 있도록 신청자, 승인자, 등록자, 등록 일시 등 관련 사항이 모두 기록될 수 있도록 하여야 하며, 위·변조 또는 분실 되지 않도록 안전하게 보관하여야 한다.

접근권한 기록에 포함되어야 할 정보 예시
● 접근권한 신청 정보 : 신청자, 신청일시, 신청 사유, 사용 기간 등 ● 접근권한 승인 정보 : 승인자, 승인/거부 여부, 승인/거부 사유, 승인/거부 일시 등 ● 접근권한 등록 정보 : 등록자, 등록일, 등록 방법 등 ● 접근권한에 관한 정보 : 권한명, 권한 내용 등 ● 기타 : 특이사항이 있는 경우 포함 (인사시스템 연계 등)

● 접근권한의 적절성에 대한 상세한 검토 및 감사가 가능하도록 검색, 조회 등의 기능을 응용프로그램의 별도 기능 또는 로그분석시스템 등으로 구현하는 것을 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.9	개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 기록하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○시스템의 접근권한 기록에 별도의 로그 테이블에 저장되어 3년간 보관되고 있으나, “승인자” 및 “등록자” 정보가 누락되어 있어 누가 승인을 하였는지 등의 정보를 사후에 파악하기 어려움				

OO시스템 접근권한 부여 기록 조회 화면	◎ 접근권한 부여 기록

◎ 접근권한 부여 기록

대상자 ID	신청일시	승인일시	발급일시	권한명	사유
excelkim	20150301	20150302	20150302	총괄관리자	인사 이동
jamesbond	20150401	20150404	20140405	운영자	인사 이동
superman	20150510	20150510	20150511	상담원	신규 입사
batman	20150510	20150510	20150511	상담원	신규 입사
...	...	...	...	...	...

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

세부분야	권한 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.10	● **개인정보처리시스템에 대한 개인정보취급자의 권한을 조회, 입력, 변경, 삭제, 출력, 다운로드 등 그 역할에 따라 최소한으로 부여할 수 있도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 목적에 필요한 최소한의 범위로 최소한의 인원에게 개인정보에 대한 접근권한을 부여하지 않은 경우				
평가근거 및 의견	● ○○기관은 내부 통합○○시스템을 이용하는 직원 중 최소한의 인원에 한하여 개인정보취급자로 지정하고 개인정보에 대한 접근권한을 부여하고 있으나, ○○팀의 ○○업무 담당자는 업무범위를 초과하는 권한을 부여하고 있음				

주요 점검 사항

1. 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 한다.
2. 개인정보를 처리하는 응용프로그램에서 업무담당자에 따라 상세하게 접근권한을 부여할 수 있도록 기능이 구현되어야 한다.
   - 권한 부여 대상 : 개인별, 그룹별, 조직별, 역할별 등
   - 권한 유형 : 조회, 입력, 변경, 삭제, 출력, 다운로드, 권한관리 등
3. 개인정보처리시스템의 서버, 데이터베이스(DB)에 대한 직접적인 접근은 운영자 및 관리자에 한정하여 최소한의 인원에게 부여하고 관리되어야 한다.

지표 해설

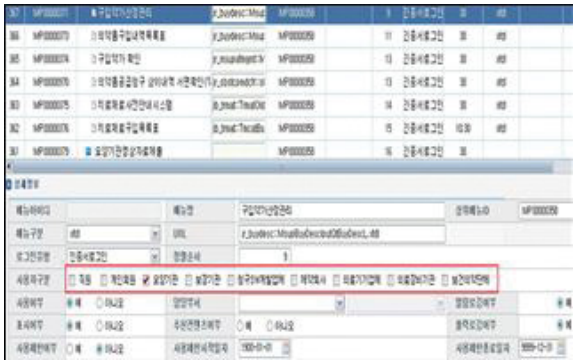
- 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 최소한의 범위로 업무담당자에게 차등 부여하고 접근통제를 위한 조치를 취하여야 한다.
  - 예를 들어, 개인정보 보호책임자에게는 전체권한(읽기/쓰기/변경)을 부여하거나, 개인정보 취급자에게는 읽기 권한만 제공하는 등 권한에 차등을 두어야 한다.

- 개인정보를 처리하기 위해 정의된 책임과 역할에 따라 개인정보처리시스템의 사용자별, 그룹별로 권한을 분리하여 정의하고, 해당 사용자별, 그룹별 권한에 따라 읽기, 쓰기, 변경 등 개인정보 처리 권한을 구분하여 정의하여야 한다.
  - 개인정보의 읽기, 쓰기, 변경 등의 권한 부여 시, 업무 목적 달성을 위한 최소한의 개인정보 항목만 읽기, 쓰기, 변경 할 수 있도록 업무별 처리하는 개인정보 항목까지 계정권한에 따라 분리하여 정의하도록 권장한다.
  - 조회 권한 부여 시에 다운로드 권한이 자동으로 부여되거나, 다운로드 권한을 설정하는 기능이 존재하지 않는 경우가 있다. 대량의 개인정보를 다운로드 받을 경우 유출의 위험성이 매우 높으므로, 다운로드 기능이 존재하는 경우 반드시 다운로드 권한을 분리하여 부여할 수 있도록 권한관리 기능을 구현하여야 한다.

- 개인정보처리시스템을 통한 개인정보 파일 다운로드, 출력 및 복사 등의 기능은 개인정보처리시스템의 접근권한을 그룹으로 분류하여 설정할 수 있으며, 그룹별 계정 발급 현황을 목록으로 관리하여 저장, 출력 및 복사의 권한 부여가 타당한지 주기적으로 점검하도록 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.10	개인정보처리시스템에 대한 개인정보취급자의 권한을 조회, 입력, 변경, 삭제, 출력, 다운로드 등 그 역할에 따라 최소한으로 부여할 수 있도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○기관은 ○○시스템 취급자에 대하여 전체적으로 업무목적에 일치하는 최소한의 범위로 접근권한을 부여하고 있음. 하지만 일부 ○○신청관리의 접근권한은 내부직원만 접근이 가능하도록 설계되어 있으나, ○○기관 담당자가 접근이 가능하도록 잘못된 권한을 부여하고 있음.				

권한부여 화면	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제5조 접근 권한의 관리

2 접근통제

세부분야	접근통제 조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.1	● **개인정보처리시스템에 대한 불법적인 접근 및 침해사고를 방지할 수 있도록 접근통제 시스템을 설치·운영하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 원격시스템으로부터의 비정상적인 개인정보 조회 또는 요청에 대해 탐지 및 차단조치를 하도록 설계하고 있는 경우				
평가근거 및 의견	● ○○시스템은 웹 환경으로 구성되어 있어 방화벽을 통해 접근 포트를 80번으로만 제한하고 있고, 웹 방화벽을 통해 실시간 모니터링 통제를 하고 있음				

주요 점검 사항

1. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근통제시스템을 설치·운영하여야 한다.
2. 해당 접근통제시스템은 아래와 같은 기능을 모두 포함하여야 한다.
   ① 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
   ② 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지 및 대응

지표 해설

- 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 접근제한, 가상사설망(VPN) 등을 이용한 안전한 접속, 인터넷 홈페이지의 취약점 점검, 업무용 컴퓨터 또는 모바일 기기의 보호조치 등 접근통제 조치가 필요하다.
- 개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 아래의 기능을 포함한 장비 설치·운영 등의 조치를 하여야 한다.

접근통제시스템 요건			
No	구분	기능	비고
1	침입차단 기능	개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한	방화벽, N/W장비 ACL 등
2	침입탐지 기능	개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지	IDS 등

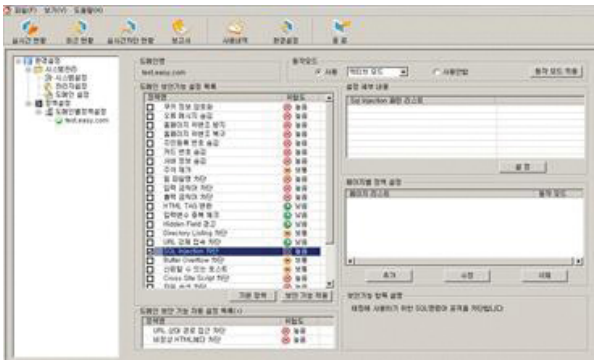
- 접근통제 요건을 만족하기 위해서는 '침입차단 기능'과 침입탐지 기능'이 모두 제공되어야 한다. 하나의 장비에서 2가지 기능을 동시에 제공할 수도 있고, 침입차단 장비와 침입탐지 장비를 조합하여 구성할 수도 있다.

침입차단 및 침입탐지 기능을 갖춘 장비의 설치 방법 예시
- 침입차단시스템, 침입탐지시스템, 침입방지시스템 등 설치·운영 - 웹 방화벽, 보안 운영체제(Secure OS) 등 도입 - 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List: 접근제어목록) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현 - 공개용 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영 - 다만, 공개용 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하고 정기적인 업데이트 여부 등 확인 후 적용 필요 - 이외에도, 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용 가능

- 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.
  - 최소권한의 원칙에 따라 서비스 제공 및 운영을 위해 필요한 IP, Port만 허용
  - 침입탐지 패턴의 최신 업데이트 및 관리
  - 특정 시간 내에 과도한 접속 시도 등 이상 행위 탐지 및 대응
  - 보안 관제 및 모니터링 체계 구축
  - 보안 로그 보존 등

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.1	개인정보처리시스템에 대한 불법적인 접근 및 침해사고를 방지할 수 있도록 접근통제 시스템을 설치·운영하도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○시스템은 웹 환경으로 구성되어 있으나 내부 직원들만 사용하도록 제한되어 있으며, 외부에서 접속이 되지 않도록 내부망에 구축되어 있음 또한 방화벽 및 웹 방화벽이 구축되어 있어 방화벽을 통해 접근포트를 80번으로만 제한하고 있고, 웹 방화벽을 통해 외부해킹에 대한 실시간 탐지 및 모니터링을 수행하고 있음				

방화벽 정책설정을 통한 서비스 접근통제	
웹 방화벽 정책 설정을 통한 웹 서비스 접근통제	

ACL_15	전체	INTERNAL	차단사이트 바이러스공격 복한차단IP	ALL	none	ANY	Deny							
ACL_16	전체	INTERNAL	차단사이트_추가	ALL	none	ANY	Deny							
ACL_17	전체	INTERNAL	불법사이트 차단사이트추가1	ALL	none	ANY	Deny							
ACL_18	전체	INTERNAL	차단사이트추가2 증권사이트	ALL	none	ANY	Deny							
설명 : 20110304_DDoS_상용메일														
ACL_19	전체	INTERNAL	차단사이트추가3 상용클라우드	ALL	none	ANY	Deny							
ACL_20	전체	INTERNAL	결격제이사이트	HTTPS NateOn HTTP	none	ANY	Deny							
ACL_21	전체	INTERNAL	모바일사이트	ALL	none	ANY	Deny							
ACL_22	전체	INTERNAL	P2P	ALL	none	ANY	Deny							

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(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 시도 탐지 및 대응

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제

세부분야	접근통제 조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.2	● **개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 개인정보 처리업무를 원격지에서 처리할 때 GVPN, VPN 등을 이용하여 암호화하도록 설계하고 있는 경우				
평가근거 및 의견	● ○○시스템은 웹 환경으로 구성되어 있고, 원격지 사업소 또는 출장업무에서 개인정보 업무처리를 위해 접근 시 VPN 망을 통해 안전하게 접근할 수 있도록 하고 있음				

주요 점검 사항

1. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

지표 해설

- 인터넷구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인 정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속 수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
- 안전한 접속 수단으로는 가상사설망(VPN: Virtual Private Network) 또는 전용선 등이 있다.

안전한 접속 수단 예시
– 가상사설망(VPN: Virtual Private Network) : 개인정보취급자가 사업장 내의 개인정보처리 시스템에 대해 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안 시스템을 의미 – 전용선 : 물리적으로 독립된 회선으로서 두 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점간 직통으로 연결하는 회선 등을 의미

- VPN은 인터넷 등 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하고 수신측에서 이를 복호화하는 방식으로 송수신 정보에 대한 기밀성 및 무결성을 보장하며, 그 외에도 데이터 출처 인증, 재전송 방지, 접근 제어 등 다양한 보안 기능을 제공한다.

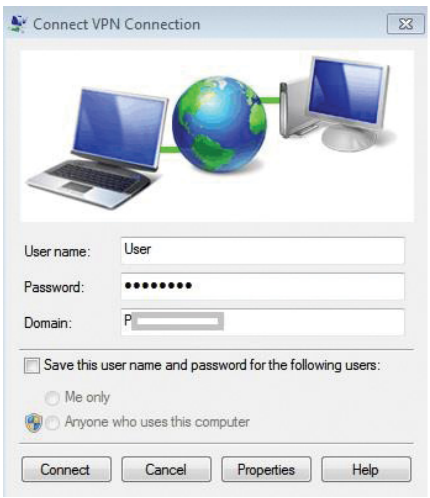
- IPSec, SSL 등의 기술이 사용된 가상사설망을 안전하게 사용하기 위해서는 알려진 취약점(예: OpenSSL의 Heart Bleed 취약점)들을 조치하여 사용할 필요가 있다. 최근에 SSL 관련 취약점이 많이 발표되는 추세에 있어 특별한 주의가 필요하다.
- 안전한 인증 수단으로는 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등이 있다.

안전한 접속 수단 예시
- 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래사실 증명, 문서의 위변조 여부 검증 등을 위해 사용하는 전자서명으로서 해당 전자사명을 생성한 자의 신원을 확인하는 수단 - 보안토큰 : 암호 연산장치 등으로 내부에 저장된 정보가 외부로 복사, 재생성되지 않도록 공동인증서 등을 안전하게 보호할 수 있는 수단으로 스마트 카드, USB 토큰 등이 해당 - 일회용 비밀번호(OTP, One Time Password) : 무작위로 생성되는 난수를 일회용 비밀번호로 한번 생성하고, 그 인증값이 한번만 사용가능하도록 하는 방식

- 인증수단만을 적용하는 경우에는 통신 보안을 위한 암호화 기술의 추가 적용이 필요할 수 있으므로, 보안성 강화를 위하여 안전한 접속수단을 권고한다.
- 인증수단에 대한 구체적인 설명은 지표 4.1.4 참조

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.2	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○시스템은 웹 환경으로 구성되어 있고, 원격지 사업소 또는 출장업무에서 개인정보 업무처리를 위해 접근 시 VPN 망을 통해 안전하게 접근할 수 있도록 하고 있음 VPN 로그인 화면				



관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(접근통제) ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제

세부분야	접근통제 조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.3	● **인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자 PC, 모바일 기기, 관리용 단말기 등에 보호 조치를 계획하고 있습니까?**	○			
평가 예시	● 이행 : 인터넷 홈페이지에 대한 취약점 점검 및 조치, 관리자 페이지 노출 차단, P2P, 웹하드, 공유설정 등 차단조치를 통해 인터넷을 통한 개인정보의 노출을 차단한 경우				
평가근거 및 의견	● A기관은 연 1회 홈페이지에 대한 정기적인 취약점 진단 및 모의해킹을 수행하고 있으며, 개인정보취급자가 인터넷을 접속하는 구간에는 DLP 및 비업무사이트 차단 솔루션을 도입하여 P2P, 웹하드 등을 통해 개인정보가 공개되거나 노출되지 않도록 보호조치를 적용하고 있음				

주요 점검 사항

1. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기, 관리용 단말기 등에 조치를 취해야 한다.
   ① 잘 알려진 웹 취약점 항목들을 포함한 웹 취약점 점검 및 조치
   ② 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL에 대한 삭제 또는 차단 조치
   ③ 인터넷 홈페이지 관리자 페이지에 대한 노출 차단 등의 보호조치
   ④ P2P, 웹 하드, 공유설정 차단 조치(단, 업무상 반드시 필요한 경우 별도의 보호대책 마련 후 허용)
   ⑤ 개인정보처리시스템은 원칙적으로 인터넷 접속 차단 조치(필요시 해당 IP 및 Port만 허용)
   ⑥ 공개된 무선망을 이용하여 개인정보를 처리하는 경우 암호화 등 개인정보 유출방지 기술 적용
   ⑦ 기타 개인정보 노출방지를 위한 조치 (웹 쉘 탐지, 첨부파일 개인정보 노출 탐지 등)

지표 해설

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 ①개인정보처리시스템, ②업무용 컴퓨터 및 ③업무용 모바일 기기, ④관리용 단말기 등에 조치를 하여야 한다.
- 취급중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 다음과 같은 항목 등을 고려하여 조치할 수 있다.

인터넷 홈페이지를 통한 개인정보 유·노출 방지 대책 예시
- 잘 알려진 웹 취약점 항목들을 포함한 웹 취약점 점검 및 조치 · 웹 취약점 점검 항목 예시 : SQL Injection, File Upload 취약점, XSS 취약점 등 · 잘 알려진 웹 취약점 점검 항목은 개인정보보호위원회, OWASP(국제웹표준기구) 등에서 발표하는 항목 참조 - 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL에 대한 삭제 또는 차단 조치 - 인터넷 홈페이지 관리자 페이지에 대한 노출 차단 등의 보호조치 - 웹 방화벽 설치·운영을 통하여 웹 해킹을 통한 개인정보 유·노출 탐지 및 차단 - 개인정보 필터링 솔루션을 통하여 게시판, 첨부파일 등을 통해 노출된 개인정보 탐지 및 변환 - 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 있음 - 개인정보처리시스템에서 인터넷으로의 아웃바운드 접속 차단(필요 시 해당 IP, Port만 허용) 등

● 또한, 취급중인 개인정보가 개인정보취급자의 업무용 컴퓨터, 모바일 기기, 관리용 단말기 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 다음과 같은 항목 등을 고려하여 조치할 수 있다.

개인정보취급자 업무용 컴퓨터 또는 모바일기기를 통한 개인정보 유·노출 방지 대책 예시
- N-DLP(Network Data Loss Prevention), 비업무사이트 차단시스템 등 보안시스템을 도입하여 개인정보의 외부전송 모니터링 및 P2P, 웹하드 등 개인정보 유·노출 위험성이 높은 사이트 차단 조치 - PC보안, E-DLP(Endpoint Data Loss Prevention) 등 업무용 컴퓨터에 보안프로그램을 설치하여 공유폴더 설정 차단, 메신저, P2P 및 웹하드 프로그램 실행차단, 매체 제어 등 조치 - 개인정보 송·수신 시 SSL, VPN 등 보안기술이 적용된 전용 프로그램을 사용하여 송·수신 또는 암호화 송·수신 - 업무용 컴퓨터, 모바일 기기에서 개인정보가 포함된 파일 송·수신 시 암호화 저장 후 송·수신 - 개인정보 유출 방지조치가 적용된 공개된 무선망 이용 (WPA2 등 보안프로토콜을 사용하는 공개된 무선망 사용 등) 등

● 개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 한다.

- 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검이 필요하다.
- 이외에도 상용 웹메일, 웹하드, 메신저, SNS 서비스 등을 통하여 고의 혹은 부주의로 인한 개인정보 유·노출 방지 조치 등이 해당될 수 있다.

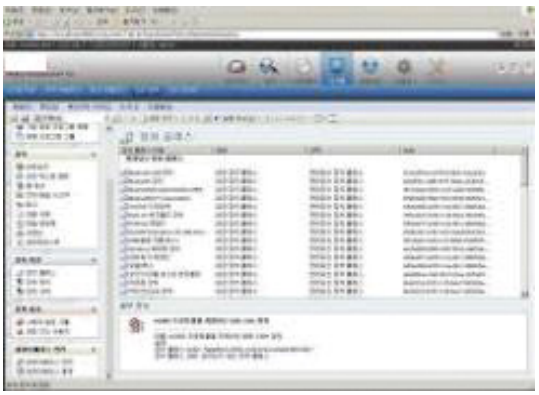
※ P2P, 웹하드 등의 사용을 제한하는 경우에도 단순히 사용금지 조치를 취하는 것이 아니라 시스템 상에서 해당 포트를 차단하는 등 근본적인 안전조치를 취하는 것이 필요하다.

- 개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 취급중인 개인정보가 신뢰 되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치의 취약점 등에 의해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 하며, 다음과 같은 방식 들을 활용 할 수 있다.
  - 비밀번호 등 송신 시 SSL, VPN 등의 보안기술이 적용된 전용 프로그램을 사용하거나 암호화하여 송신한다.
    ※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 개인정보 전송시, 전송 암호화 기능이 탑재된 별도의 앱(App)이나 프로그램을 설치하고 이를 이용하여 전송
  - 고유식별정보 등이 포함된 파일 송신 시 파일을 암호화하여 저장 후 송신한다.
    ※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 고유식별정보가 포함된 파일 송신 시, 암호화 저장 한 후 송신
  - 개인정보 유출 방지 조치가 적용된 공개된 무선망을 이용한다.
    ※ 예시: 모바일 기기, 노트북에서 설치자를 신뢰할 수 있고 관리자 비밀번호 등을 포함한 알려진 보안취약점이 조치된 무선접속장치에 안전한 비밀번호를 적용한 WPA2(Wi-Fi Protected Access 2) 보안 프로토콜을 사용하는 공개된 무선망 사용

- 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통한 개인정보의 유·노출을 방지하기 위한 방법은 반드시 위에서 제시된 방법이 모두 적용되어야 하는 것은 아니며, 최신의 위협 동향, 대상 시스템 및 대상 기관의 특성, 위험도 등을 고려하여 적절한 방법과 수준을 결정할 수 있다. 다만, 이러한 방법과 수준을 결정할 때에는 개인정보처리시스템, 업무용 컴퓨터, 업무용 모바일기기, 관리용 단말기의 4가지 영역이 모두 고려될 수 있도록 하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.3	인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자 PC, 모바일 기기, 관리용 단말기 등에 보호 조치를 계획하고 있습니까?	○			
평가근거 및 의견	● A 기관은 홈페이지에 대한 정기적인 취약점진단 및 모의해킹을 수행하고 있음(2016년 2월에 ○○○보안 전문업체를 통하여 홈페이지 취약점 진단 수행). 또한 DLP 솔루션 도입을 통해 이메일, 인스턴트메신저, FTP, HTTP 등을 통한 개인정보 외부전송을 통제하고 있으며, 유해차단 시스템을 구축하여 유해사이트, P2P 등에 대한 보호를 수행하고 있음 (단, 업무용 모바일 기기는 사용하지 않고 있음)				

DLP 솔루션 도입을 통한 접근통제	
유해차단 시스템을 통한 유해사이트 차단	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(접근통제) ③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제
- 홈페이지 개인정보 노출방지 가이드라인

세부분야	접근통제 조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.4	● **개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대한 안전조치를 적용하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 관리용 단말기를 별도로 운영하여 인터넷 차단 등 보호조치를 수행하고 다른 목적으로 사용하고 있지 않는 경우				
평가근거 및 의견	● A기관은 개인정보처리시스템 운영 및 유지보수를 위해 관리용 단말기를 별도로 준비하고 있으며, 네트워크 분리, 인터넷 사용 통제, USB 사용 통제 등 안전조치를 적용하여 관리하고 있음				

주요 점검 사항

1. 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치를 하여야 한다.
   ① 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
   ② 본래 목적 외로 사용되지 않도록 조치
   ③ 악성프로그램 감염 방지 등을 위한 보안조치 적용

지표 해설

- 개인정보처리자는 관리용 단말기에 대해 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 업무처리를 하는 특정 직원 등에 한하여 접근을 허용하는 등 업무관련자 이외의 인가 받지 않는 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 접근통제 등의 안전조치를 하여야 한다.
- 개인정보처리자는 관리용 단말기를 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 사용 하여야 하며, 관리용 단말기를 통한 개인정보의 공유 등 다른 목적으로 사용하지 않아야 한다.
- 개인정보처리자는 관리용 단말기에 대하여 악성프로그램 감염 방지를 위한 보안 프로그램의 최신상태 유지, 보안 업데이트 실시, 발견된 악성프로그램의 삭제 등 대응 조치 등을 적용하여야 한다.

관리용 단말기의 안전조치 예시
- 관리용 단말기 현황 관리(IP주소, 용도, 담당자, 설치 위치 등) - 중요 관리용 단말기를 지정하여 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 - 관리용 단말기에 주요 정보 보관 및 공유 금지 - 비인가자 접근을 방지하기 위한 부팅암호, 로그인 암호, 화면보호기 암호 설정 - 보조기억매체 및 휴대용 전산장비 등에 대한 접근 통제 - 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지 - 악성코드 감염 방지를 위한 보안 프로그램의 최신상태 유지, 보안 업데이트 적용, 악성프로그램 삭제 등 대응 조치 - 보안 상태 및 사용현황에 대한 정기 점검

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.4	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대한 안전 조치를 적용하도록 계획하고 있습니까?	○			
평가근거 및 의견	● A기관은 개인정보처리시스템 운영 및 유지보수를 위해 관리용 단말기를 별도로 준비하고 있으며, 네트워크 분리, 인터넷 사용 통제, USB 사용 통제 등 안전조치를 적용하여 관리하고 있음 관리적 단말기 운영 현황				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제10조 관리용 단말기의 안전조치

세부분야	인터넷 홈페이지 보호조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.5	● **인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용 프로그램에 대한 취약점 점검 및 대응조치를 적용하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 인터넷 홈페이지에 대한 취약점 점검을 수행하였으나, 일부 영역(웹서버 등)에 대하여 점검 범위에서 빠져 있거나, 발견된 취약점에 대한 개선조치 계획이 수립되어 있지 않은 경우				
평가근거 및 의견	● ○○○기관 인터넷 홈페이지에 대한 취약점 진단 결과 10개의 취약점이 발견되었으나, 이에 대한 개선조치 계획을 수립하지 않음				

주요 점검 사항

1. [개발 시]인터넷 홈페이지 취약점으로 인한 개인정보 침해를 방지하기 위한 시큐어 코딩, 취약점 점검 등의 개발보안 조치가 적용되어야 한다.
   ※ '행정기관 및 공공기관 정보시스템 구축·운영 지침'에 따른 개발보안 대상 정보화사업의 경우, 고유식별정보 처리 여부와 무관하게 SW보안약점 점검 수행 필요
2. [운영 시]인터넷 홈페이지에 대한 정기 취약점 진단 계획을 수립하고 이행하여야 하며, 특히 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우에는 인터넷 홈페이지에 대하여 연 1회 이상 취약점을 점검하여야 한다.
3. 취약점 점검 대상은 인터넷 홈페이지와 관련된 정보자산(응용프로그램, 웹서버 등)을 모두 포함하여야 한다.
4. 취약점 점검에서 발견된 취약점은 개선 계획을 수립하고, 해당 계획에 따라 개선이 될 수 있도록 지속적으로 관리하여야 한다.(이행 점검 등)

지표 해설

- 개인정보를 처리하는 인터넷 홈페이지의 경우 불특정 다수가 접근할 수 있는 특성으로 인하여 직접적인 해킹 공격의 위협에 노출되어 있다. 따라서, 개발단계부터 보안이 고려되고 적용되어 안전하게 운영할 수 있는 기반을 마련하는 것이 매우 중요하다고 하겠다.
- 개인정보처리시스템을 신규로 개발하는 경우에는 분석·설계 단계에서 개인정보보호 및 보안 측면에서 요구사항을 명확히 정의하여 설계에 반영하고, 개발 단계에서는 해당 요건에 따라 안전한 프로그래밍(시큐어 코딩)이 적용되어야 하며, 테스트 단계에서 보안 요건의 반영여부 및 취약점 존재여부를 점검·조치하여 안전한 상태로 시스템이 오픈될 수 있도록 개발보안 절차를 마련하여 적용하는 것이 권장된다.
- 「개인정보의 안전성 확보조치 기준 고시」에 따르면 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 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 고유식별정보 등의 유출·변조·훼손의 위험을 더욱 줄일 수 있다.

● 참고적으로 대상 정보화 사업이 정보시스템 감리대상 요건에 해당될 경우에는 '행정기관 및 공공기관 정보시스템 구축·운영 지침(행정안전부 고시, 2019.8)'에 따라서 SW 보안약점에 대한 점검을 수행하여야 하므로, 대상 사업이 요건에 해당하는지 확인이 필요하다.

● 웹 취약점 점검 시에는 개인정보보호위원회, OWASP(국제 웹표준 기구), 국가 사이버안전센터 (NCSC) 등에서 발표하는 항목을 참고하여 잘 알려진 웹 취약점 항목들이 포함되도록 할 필요가 있다.

【소프트웨어 보안약점 유형】(소프트웨어 개발보안 가이드, 행정안전부)

유형	내용	갯수
입력데이터 검증 및 표현	- 프로그램 입력값에 대한 검증 누락 또는 부적적한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점 (예) SQL삽입, 정로 조작 및 자원 삽입, 크로스사이트 스크립트 등	15
보안기능	- 보안기능(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 적절하지 않게 구현시 발생할 수 있는 보안약점 (예) 부적절한 인가, 중요정보 평문저장, 하드코드된 비밀번호 등	16
시간 및 상태	- 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작되는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안약점 (예) 경쟁조건 : 검시시점과 사용시점(TOCTOU) 등	2
에러처리	- 에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점	3
코드오류	- 타입 변환 오류, 자원(메모리)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩 오류로 인해 유발되는 보안약점 (예) Null Pointer 역참조, 부적절한 자원 해제 등	4
캡슐화	- 중요한 데이터 또는 기능성을 불충분하게 캡슐화 하였을 때 인가되지 않은 사용자에게 데이터 누출이 가능해지는 취약점 (예) 제거되지 않고 남은 디버거 코드, 시스템 데이터 정보노출 등	5
API 요용	- 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점 (예) DNS lookup에 의존한 보안결정 등	2

【OWASP TOP 10】(2020년 발표)

구분	설명
A1	인젝션
A2	취약한 인증
A3	기밀 데이터의 노출
A4	XML 외부 객체(XEE)
A5	취약한 접근통제
A6	보안 설정 오류
A7	크로스사이트스크립팅(XSS)
A8	불안정한 Deserialization
A9	기존에 알려진 취약성을 가진 Component의 사용
A10	불충분한 로깅 및 모니터링

【국정원 8대 취약점】

구분	설명
1	디렉토리 리스팅 취약점
2	파일 다운로드 취약점
3	파일 업로드 취약점
4	크로사이트 스크립팅(XSS) – OWASP TOP 10과 동일
5	Web DAV 취약점
6	TechNote 취약점
7	Zeroboard 취약점
8	SQL 인젝션 취약점 – OWASP TOP 10과 동일

- 또한, 최근의 해킹 공격들이 단순히 웹 프로그램의 취약점 뿐만 아니라 웹서버, 오픈소스 (OpenSSL 등), 운영체제(OS)의 취약점을 이용하는 경우가 증가하고 있으므로, 취약점 점검 시 웹 서버(OS), 웹패키지 S/W(WAS 등), 네트워크 장비, DB 등 인터넷 홈페이지와 관련된 정보자산은 모두 점검대상에 포함할 필요가 있다.
- 인터넷 홈페이지의 취약점 점검 시에는 기록을 남겨 책임 추적성 확보 및 향후 개선조치 등에 활용할 수 있도록 하는 것이 바람직하다.
- 인터넷 홈페이지의 취약점 점검은 개인정보처리자의 자체 인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 활용할 수 있다.
- 취약점 점검 결과에 따라 발견된 취약점에 대해서는 이행조치 계획을 수립하고, 실제 이행 여부를 재점검하는 계획을 수립할 것을 권장한다.
- 인터넷 홈페이지뿐만 아니라, 모바일을 기반으로 대민서비스를 제공하는 경우에도 취약점 점검 및 조치를 수행하여 안전하게 모바일 서비스가 운영될 수 있도록 할 필요가 있다. ('모바일 대민서비스 보안취약점 점검 가이드' 등 참고)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.5	인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용 프로그램에 대한 취약점 점검 및 대응조치를 적용하도록 계획하고 있습니까?	○			
평가근거 및 의견	● 행정안전부 '홈페이지 SW(웹) 개발보안 가이드'에 따라 개발은 진행하고, 개발한 ○○시스템에 대한 웹 취약점 점검을 수행하여 취약한 부분은 보완조치를 수행함 취약점 결과 보고서 ○○시스템 취약점 분석·평가 **웹 취약점 진단 보고서** 2013. 2.				

	취약한 내역 조치결과 공문	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(접근통제) ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제
- 소프트웨어 개발보안 가이드(2019.11, 행정안전부)
- 소프트웨어 보안약점 진단가이드(2019.6, 행정안전부)
- 모바일 대민서비스 보안취약점 점검 가이드(2015.12, 행정안전부)
- 홈페이지 개인정보 노출방지 안내서(2018.11, 행정안전부)
- 홈페이지 취약점 진단·제거 가이드(2013, KISA)
- 웹 서버 구축 보안점검 안내서(2010, 방송통신위원회)

세부분야	업무용 모바일기기 보호조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.2.6	● 개인정보를 처리하는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?	○			
평가 예시	● 이행 : 업무용 모바일 기기의 분실·도난 등으로 인한 개인정보 유출을 방지하기 위하여, 업무용 모바일 기기에 비밀번호를 사용하여 화면 잠금 설정 등을 한 경우				
평가근거 및 의견	● ○○○기관은 업무용 모바일기기에 MDM솔루션을 설치하여 비밀번호 화면잠금 설정, 분실 시 원격 데이터삭제 등의 기능을 적용함				

주요 점검 사항

1. 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 적용하여야 한다.
2. 고유식별정보 또는 민감한 개인정보를 처리하는 업무용 모바일 기기는 해당 개인정보의 유출을 방지하기 위하여 강화된 보호조치를 적용하여야 한다.
   ① 데이터 암호화
   ② 분실 시 대책(원격 잠금, 원격 데이터 삭제 등)
   ③ 기타 보호조치(기기 인증, 루팅 통제 등)

지표 해설

- ‘모바일 기기’라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿 PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
- 최근 업무용 모바일 기기는 성능이 높아 대량의 개인정보를 저장하거나 전송할 수 있으나, 휴대와 이용이 편리하여 기기 분실·도난 시 해당 기기에 저장된 또는 해당 기기의 정보처리시스템 접속 등을 통한 개인정보 유출의 위험성이 높다.
- 따라서, 스마트폰, 태블릿PC와 같이 개인정보 처리 업무에 사용되는 모바일 기기는 분실·도난으로 개인정보가 유출되지 않도록 개인정보처리자의 기기 운영 환경 및 처리되는 개인정보의 중요도 등을 고려하여 아래와 같은 항목들을 조치 항목으로 고려할 수 있다.

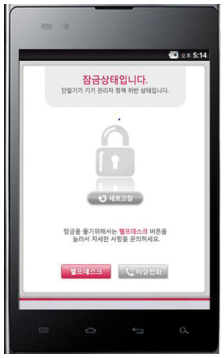
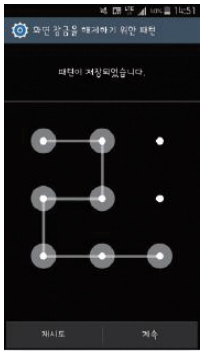
  - 비밀번호, 패턴, PIN 등을 사용하여 화면 잠금 설정
  - 디바이스 암호화로 애플리케이션, 데이터 등 암호화

- USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금설정
- 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 등의 조치 (제조사별로 지원하는 '킬스위치 서비스'나 이동통신사의 '잠금앱 서비스' 등)

  ※ 업무용 모바일 기기 분실 시, 신고 및 대응 절차(원격 데이터 삭제, 통신사 분실 신고, 개인정보처리시스템 접속 차단 조치 등)를 마련하여 이행할 필요가 있음

● 고유식별정보, 민감정보 등 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 루팅 등 단말변경 통제, 접속 통제 등의 강화된 보호조치를 적용하는 것이 권장된다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.2.6	개인정보를 처리하는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?	○			
평가근거 및 의견	● ○○○기관은 현장 민원처리 업무를 위해 일부 담당자들이 모바일기기를 사용하고 있으며, 모바일 기기 분실·도난 등으로 인한 개인정보유출을 방지하여 위하여 별도의 모바일뷰어 솔루션을 활용하여 모바일 기기에는 데이터가 저장되지 않도록 하고 있으며, MDM솔루션을 적용하여 화면 잠금 강제화 등의 보호조치를 적용함 모바일기기 MDM 설치 및 화면잠금 화면  				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제6조(접근통제) ⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제6조 접근통제

3 개인정보의 암호화

세부분야	저장 시 암호화				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.3.1	● **고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 중요 개인정보를 저장·보유 시 암호화를 하고 있으나, 안전한 알고리즘을 사용하지 않은 경우				
평가근거 및 의견	● ○○연수원 학사관리시스템은 외부강사의 강사료 지급업무와 관련된 ○○ 개인정보파일을 운용하고 있으며, 주민등록번호와 비밀번호의 중요 개인정보를 암호화하여 저장·보유하고 있으나 주민등록번호는 ARIA로 안전한 알고리즘을, 비밀번호는 MD5방식의 안전하지 않은 일방향 암고리즘을 사용하고 있음				

주요 점검 사항

1. 비밀번호는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다.
2. 주민등록번호 및 바이오정보는 저장 위치와 상관없이 암호화하여 저장하여야 한다.
   ※ 단, 주민등록번호에 대해서는 100만건 미만일 경우 2017년 1월 1일까지, 100만건 이상일 경우 2018년 1월 1일까지 암호화 조치 완료 필요
3. 고유식별정보(주민등록번호 제외)를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점 (DMZ)에 저장하는 경우에는 이를 암호화하여야 한다.
4. 고유식별정보(주민등록번호 제외)를 내부망에 저장하는 경우에는 암호화를 적용하거나 위험도 분석에 따른 결과에 따라 암호화 적용여부 및 적용여부를 정하여 시행할 수 있다.
   ※ 위험도 분석은 공식적인 절차를 통해 수행되어야 함
5. 암호화는 안전한 방식으로 적용되어야 한다.
   ① 안전한 알고리즘 사용
   ② 암호화키의 유·노출을 방지하기 위한 안전한 키관리
   ③ 비밀번호 일방향 암호화 시 Salt값 적용 등(권고 사항)
6. 업무용 컴퓨터, 모바일 기기에 고유식별정보, 비밀번호, 바이오정보를 저장하는 경우 상용 암호화소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.
   ※ 신용정보보호법 등 타 법령 적용 대상일 경우, 해당 법령에서 요구하는 암호화 대상 및 방법 준수 필요

지표 해설

- 암호화는 개인정보취급자의 실수 또는 외부 공격자(해커)의 공격 등으로 인해 개인정보가 비인가자에게 유·노출되더라도 그 주요 내용을 확인할 수 없게 하는 보안기술을 의미한다. 주요 개인정보가 암호화되지 않고 개인정보처리시스템에 저장되거나 네트워크를 통해 전송될 경우, 불법적인 노출 및 위·변조 등의 위험이 있으므로 암호화 등의 안전한 보호조치가 제공되어야 한다.

- 「개인정보 보호법」에 따라 암호화 대상이 되는 개인정보는 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호), 비밀번호, 바이오정보이다. 참고적으로 정보통신서비스 제공자등은 「개인정보의 기술적·관리적 보호조치 기준」에 따라 고유식별정보, 비밀번호, 바이오정보 외에도 금융정보에 해당하는 카드번호, 계좌번호도 저장 시 암호화 대상으로 규정하고 있으므로 대상 기관 및 대상 시스템이 적용받는 법률 상에 암호화 관련 요건이 있는지 파악하여 적용할 필요가 있다.

- 비밀번호의 경우에는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다. 참고적으로 일방향 암호화는 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수(해시 함수 등)에 적용하여 얻는 결과값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.

- 다만, 비밀번호를 해시함수를 통하여 단순히 일방향 암호화만 하는 경우에는 동일한 비밀번호를 사용하는 사용자는 동일한 해시값을 가지게 되며, 레인보우 테이블을 이용하면 해시값으로부터 비밀번호를 쉽게 추출해 낼 수 있는 위험이 존재한다. 따라서 비밀번호를 일방향 암호화 할 때에는 Salt값 적용 등의 방법으로 안전하게 일방향 암호화를 적용할 필요가 있다.

  - '레인보우 테이블'이란 해시 함수를 사용하여 변환 가능한 모든 해시 값을 저장시켜 놓은 표를 말하며, 일반적으로 해시 함수를 이용하여 저장된 비밀번호로부터 원래의 비밀번호를 추출해 내는데 사용된다.

  - 'Salt값'이란 동일한 비밀번호에도 다른 해시값이 나오도록 하기 위하여 해시함수를 적용하기 전에 비밀번호에 덧붙이는 임의의 값을 말한다. 이러한 Salt값은 해당 사용자에게만 관련된 고유값이나 랜덤값 등을 이용하여 사용자마다 다르게 적용되어야 한다.

- 주민등록번호 및 바이오정보는 저장 위치 및 위험도 분석 결과와 상관없이 암호화하여 저장하여야 한다. 단 주민등록번호의 암호화 적용 시기는 「개인정보 보호법 시행령」 제21조의2제2항에 따라 아래와 같다.

  - 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자 : 2017년1월1일
  - 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자 : 2018년1월1일

- 주민등록번호에 대해서는 시스템 성능 등의 사유로 전체 암호화가 어려운 경우에는 주민등록번호의 일부분만 암호화하는 부분암호화를 적용할 수 있다. 이 경우 주민등록번호 뒤 6자리는 반드시 암호화될 수 있도록 하여야 한다.

- 바이오정보의 경우 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담 시 저장되는 음성기록이나 일반 사진정보는 암호화 대상에서 제외된다.

- 고유식별정보(주민등록번호 제외)를 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점 (DMZ)에 저장하는 경우에는 이를 암호화하여야 한다.

- 고유식별정보(주민등록번호 제외)를 내부망에 저장하는 경우에는 개인정보 영향평가 및 위험도 분석결과에 따라 암호화 적용여부 및 적용범위를 정하여 시행할 수 있다. 여기서 '위험도 분석'은 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 유출 시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

  - '위험도 분석'은 개인정보 위험도 분석 기준에 따라 수행되어야 하며 정책기반, 네트워크 기반, DB 및 Application 기반, 웹 기반의 4개 영역 총 26개 점검항목을 모두 준수할 경우 내부망에 저장된 고유식별정보에 대하여 암호화를 하지 않을 수 있다.

  - '위험도 분석'은 개인정보를 저장하는 정보시스템에서 개인정보파일 단위로 수행하고 각 개별 개인정보파일의 위험점수에 따라 개별 개인정보파일 단위로 암호화 여부를 결정해야 하며, 위험도 분석을 수행한 결과는 최고경영층으로부터 내부결재 등의 승인을 받아야 한다.

  - 개인정보 영향평가를 수행할 때에도 내부망에 저장된 고유식별정보의 암호화 적용 여부 및 적용범위를 정하기 위하여 「개인정보 위험도 분석 기준」에 따라서 위험도 분석을 수행할 수 있다.

- DBMS에 저장된 개인정보를 암호화 할 때에는 '개인정보 암호화 조치 안내서'를 참조하여 다음과 같은 방법을 선택하거나, 두 가지 이상의 방법을 혼합하여 암호화 할 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.

개인정보처리시스템 암호화 방식의 구분			
방식	암·복호화 모듈위치	암·복호화 요청위치	주요 내용
응용 프로그램 자체 암호화	어플리케이션 서버	응용 프로그램	- 암·복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고, 응용 프로그램에서 해당 암·복호화 모듈을 호출하는 방식 - DB 서버에 영향을 주지 않아 DB서버의 성능 저하가 적은 편이지만 구축 시 응용프로그램 전체 또는 일부 수정 필요 - 기존 API 방식과 유사

개인정보처리시스템 암호화 방식의 구분			
방식	암·복호화 모듈위치	암·복호화 요청위치	주요 내용
DB서버 암호화	DB 서버	DB 서버	- 암·복호화 모듈이 DB 서버에 설치되고 DB서버에서 암·복호화 모듈을 호출하는 방식 - 구축 시 응용프로그램의 수정을 최소화할 수 있으나 DB서버에 부하가 발생하며 DB 스키마의 추가 필요 - 기존 Plug-in 방식과 유사
DBMS 자체 암호화	DB 서버	DBMS 엔진	- DB서버의 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
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 응용 프로그램의 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

- 공공기관에서 DB암호화 제품을 도입하는 경우에는 「전자정부법」 등에 따라 국가정보원이 안전성을 확인한 암호모듈 또는 제품을 우선 적용하여야 한다.

- 암호화를 하는 경우에는 안전한 알고리즘을 적용하여야 한다. 안전한 알고리즘의 기준은 아래 사항을 참고할 수 있으나, IT기술의 발전에 따라 변할 수 있으므로 암호화 적용 시점에 국내외 암호전문기관의 최신정보를 반드시 확인하도록 한다.

안전한 암호 알고리즘 (예시)	
구 분	알고리즘 명칭
대칭키 암호 알고리즘	● SEED ● ARIA-128 이상(ARIA-128/192/256 등) ● AES-128 이상(AES-128/192/256 등) ● Blowfish, Camelia-128/192/256 등 ※ DES, 3DES는 안전하지 않으므로 사용하지 않아야 함
공개키 암호 알고리즘	● RSA (2048 bit 이상) ● KCDSA 등
일방향 암호 알고리즘	● SHA-2 이상(SHA-224/256/384/512 등) ※ MD5, SHA-1은 안전하지 않으므로 사용하지 않아야 함

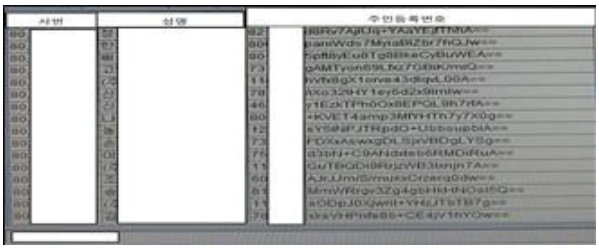
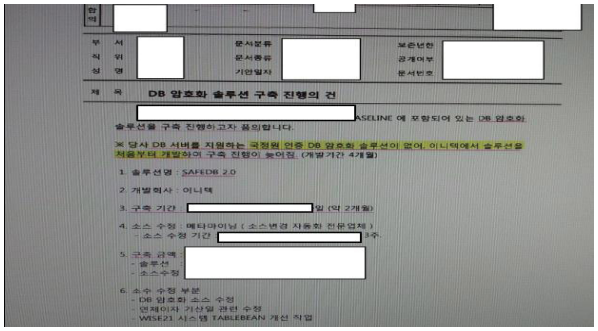
● DB 암호화의 안전성을 확보하기 위해서는 안전한 암호키의 관리가 필요하다. 암호화된 개인정보가 유출되더라도 복호화 할 수 없도록 암호키에 대한 추가적인 보안과 제한된 관리자만 허용하도록 하는 기술의 적용하여야 한다. 특히 응용프로그램 소스코드 내에 암호키가 평문으로 포함되지 않도록 하여야 한다.

● 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

- 문서도구 자체 암호화 : 한컴 오피스, MS 오피스 등에서 제공하는 암호 설절 기능 활용
- 암호 유틸리티를 이용한 암호화 : 파일 암호화 전용 유틸리티 이용
- DRM(Digital Right Management) : 문서보안 솔루션을 이용한 암호화
- 디스크 암호화 : 디스크에 데이터를 기록할 때 자동으로 암호화 등

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.3.1	고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○연수원 학사관리시스템은 외부강사의 강사료 지급업무와 관련된 ○○ 개인정보파일을 운용하고 있으며, 주민등록번호와 비밀번호의 중요 개인정보를 암호화하여 저장·보유하고 있으나 주민등록번호는 솔루션을 도입하여 ARIA로 안전한 알고리즘을 적용하였으나, 비밀번호는 MD5 방식의 안전하지 않은 일방향 알고리즘을 사용하고 있음.				

	주민등록번호 암호화 (ARIA)	  DB 암호화 솔루션 구축 진행의 건
	주민등록번호 암호화 (ARIA)	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제23조(민감정보의 처리 제한) 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.

제24조(고유식별정보의 처리 제한) 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.

제24조의2(주민등록번호 처리의 제한) 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.

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.

【개인정보 보호법 시행령】

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 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 보호위원회는 기술적· 경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

제30조(개인정보의 안전성 확보조치) 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 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여

송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 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. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제7조 개인정보의 암호화
- 개인정보 암호화 조치 안내서(2017, 행정안전부)
- 개인정보 위험도 분석 기준 및 해설서(2012, 행정안전부)
- 암호기술 구현 안내서(2013, KISA)

세부분야	저장 시 암호화				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.3.2	● **암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 암호화된 개인정보를 안전하게 보관하기 위해 암호키 관련 절차는 마련되어 있으나 시행되고 있지 않는 경우				
평가근거 및 의견	● ○○기관 개인정보보호 관련 부서에서 개인정보의 안전성확보를 위해 고유식별정보 등을 암호화하여 적용하고 있고, 이에 대한 암호 키 관리절차를 수립하고 있으나, 절차에 따른 암호키 관리는 수행되고 있지 않음				

주요 점검 사항

1. 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

지표 해설

- 개인정보처리자는 개인정보처리시스템에서 민감한 정보를 안전하게 보관하고 전송하기 위해 정보를 암호화하여야 한다. 하지만 암호화만으로는 정보의 안전성을 보장할 수 없다. 암호화된 정보의 안전성은 암호 알고리즘뿐만 아니라 키의 보안 강도, 키와 관련된 매커니즘 및 프로토콜의 효율성, 키에 대한 보호 조치 등과도 연관이 있다. 만약 암호 키에 대한 관리 소홀로 암호 키가 유출된다면, 암호화를 통한 정보보호의 의미가 없을 것이다. 따라서 암호 키에 대한 철저한 관리가 필요하다. 모든 암호 키는 변조, 도난, 유출 되어서는 안된다. 이 모든 것을 포함하여 암호 키를 안전하게 보관하고 사용하기 위해 필요한 것이 '키 관리' 이다.

- 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립·시행하여야 한다.

암호 키 관리 (예시)	
구 분	설 명
1. 준비 단계 (암호키가 생성되기 이전의 단계)	- 암호 키 생성 · 암호 키 생성에 필요한 난수는 안전한 난수발생기(RNG)를 이용하여 생성 · 비대칭키 알고리즘 키 생성 방식: 디지털 서명을 위한 키 쌍 생성, 키 설정을 위한 키 쌍 생성 · 대칭키 알고리즘 방식: 미리 공유된 키, 패스워드, 다수의 암호 키를 이용한 키 생성 등 - 암호 키 분배 · 대칭키 알고리즘 키 분배 방식: 수동적 키 분배, 자동화된 키 전송 등 · 비대칭키 알고리즘의 키 분배 방식 · 기타 키 자료 생성 및 분배 방식: 영역 파라미터, 초기값, 공유된 비밀, RNG 시드, 다른 공개 및 비밀정보, 중간 값, 난수, 패스워드 등
2. 운영 단계 (암호 키가 암호 알고리즘 및 연산에 사용되는 단계)	- 암호 키의 유효기간동안 사용되는 키 자료들은 필요에 따라 장비 모듈에 보관되거나 별도의 저장 매체에 보관 등으로 저장해야 함 - 암호 키는 하드웨어 손상 또는 소프트웨어 오류 등의 사유로 손상될 가능성이 있으므로 가용성 보장을 위해서는 키 백업 및 키 복구 등이 가능해야 함 - 암호 키가 노출되거나 노출의 위협이 있는 경우 그리고 암호키 유효기간의 만료가 가까워지는 경우에는 암호 키를 다른 암호키로 안전하게 변경해야 함
3. 정지 단계 (암호 키가 더 이상 사용되지 않지만, 암호 키에 대한 접근은 가능한 단계)	- 암호 키 보관 및 복구 · 암호 키는 수정이 불가한 상태이거나 새로운 보관 키를 이용하여 주기적으로 암호화 · 운영 데이터와 분리되어 보관하며, 암호 정보의 사본들은 물리적으로 분리된 곳에 보관 · 암호 키는 응용프로그램의 소스 프로그램 내에 평문으로 저장 금지 · 암호화되는 중요한 정보에 대한 보관키는 백업되어야 하며, 사본은 다른 곳에 보관 등 - 모든 개인키나 대칭키의 복사본이 더 이상 필요하지 않다면 즉시 파기하여야 함 - 암호 키 손상시 유효기간 내에 키 자료를 제거하고, 보안 도메인에 속해있는 실체의 권한을 삭제하여 말소된 실체의 키 자료의 사용을 방지해야 함
4. 폐기 단계 (암호 키가 더 이상 사용될 수 없는 단계 (폐기 또는 사고 상태))	- 일반적으로 폐기 단계의 키 자료에 대한 모든 기록은 삭제(다만, 일부기관에서는 감사를 목적으로 특정 키 속성 유지가 필요할 수도 있음) - 폐기 상태의 암호 키와 사고 상태의 암호 키들의 특성에 대한 기록 유지 등

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.3.2	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○기관 개인정보보호 관련 부서에서 개인정보의 안전성확보를 위해 고유식별정보 등을 암호화하여 적용하고 있고, 이에 대한 암호 키 관리절차를 수립하고 있으나, 절차에 따른 암호키 관리는 수행되고 있지 않음				

암호키 관리 지침	암호 키 관리 보안 절차 2017. 2.	1. 개요 가. 목적 나. 적용범위 2. 암호프로그램 및 암호 키 관리 가. 관리적 보안 나. 기술적 보안

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

제30조(개인정보의 안전성 확보조치) 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 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제7조(개인정보의 암호화)

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제7조 개인정보의 암호화
- 개인정보 암호화 조치 안내서(2017, 행정안전부)
- 암호 키 관리 안내서(2014, KISA)

세부분야	저장 시 암호화				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.3.3	● **고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 사용자의 PC로부터 웹서버구간의 중요 개인정보 전송 시 암호화를 적용하도록 설계문서에서 확인할 수 있으나, 일부구간 또는 일부기능에만 적용하고 있는 경우				
평가근거 및 의견	● ○○시스템에서 중요 개인정보 수집 시 SSL방식으로 암호화를 하여 안전하게 전송을 하고 있으나, IP/PW 찾기 본인인증, 회원가입 등 일부 기능에서는 평문으로 전송하고 있음				

주요 점검 사항

1. 고유식별정보, 바이오정보, 비밀번호를 정보통신망을 통하여 송·수신하는 경우 이를 암호화하여야 한다.
2. 고유식별정보, 바이오정보, 비밀번호를 보조저장매체 등을 통하여 전달하는 경우 이를 암호화하여야 한다.
3. 인터넷 등 공개된 정보통신망을 통해 개인정보를 송·수신하는 경우 이를 암호화하여야 한다. (권고 사항)

※ 정보통신망이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말함

※ 신용정보보호법 등 타 법령 적용 대상일 경우, 해당 법령에서 요구하는 암호화 대상 및 방법 준수 필요

지표 해설

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보 등을 정보통신망을 통하여 송·수신하는 경우 이를 암호화하여야 한다. 암호화를 할 때에는 아래와 같은 방법을 적용할 수 있다.

  - SSL(Secure Socket Layer) 방식
  - 암호화 응용프로그램(솔루션) 방식
  - IPSec VPN 또는 SSL VPN 방식
  - 첨부문서 암호화 후 이메일 등으로 전송하는 방식 등

- 웹브라우저가 SSL 방식으로 웹서버에 연결된 경우에는 아래와 같이 웹브라우저 주소창 또는 하단의 상태 표시줄에 자물쇠 표시가 나타나게 된다.

SSL 방식에서 나타나는 웹브라우저 자물쇠 표시 (예시)		
Internet Explorer의 경우	Chrome의 경우	FireFox의 경우
※ 웹브라우저 버전별로 표시 방식이 다를 수 있음		

- 최근 DROWN, CacheBleed, HeartBleed 등 SSL 관련 취약점들이 지속적으로 발견되고 있으므로, SSL 방식을 사용할 경우에는 최신의 취약점 정보를 확인하여 안전하게 설정할 수 있도록 하여야 한다.

- 전송 구간 암호화 적용여부를 확인하기 위해서는 Wireshark와 같은 네트워크 스니핑 도구를 활용하여 네트워크로 전송되는 데이터를 캡쳐하여 확인하는 방법이 일반적으로 활용된다.

- 고유식별정보, 비밀번호, 바이오정보 이외의 개인정보도 인터넷 등 공개망을 통해 전송되는 경우에는 비인가자에 의해 전송 데이터가 유 · 노출될 가능성이 높으므로 가급적 암호화하여 전송할 것을 권고한다. (인터넷 홈페이지 회원정보 조회 · 변경 화면 등)

  - 참고로 정보통신서비스제공자 등은 정보통신망을 통해 「개인정보의 기술적·관리적 보호조치 기준」에 따라 "개인정보"를 송수신하는 경우에는 이를 필수적으로 암호화하여야 한다.

- 보조저장매체를 통해 고유식별정보, 비밀번호, 바이오정보를 전달하는 경우에도 암호화 하여야 하며 이를 위해 다음과 같은 방법이 사용될 수 있다.

  - 암호화 기능을 제공하는 보안USB 등의 보조저장매체에 저장하여 전달
  - 해당 개인정보를 암호화 저장 후 보조저장매체에 저장하여 전달

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.3.3	고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하도록 계획하고 있습니까?		○		

평가근거 및 의견

- ○○시스템 로그인 페이지에는 https(SSL) 암호화 통신은 적용되어 동작하고 있으나, 그 외 개인정보를 수집하여 송·수신하는 회원관리 화면에는 암호화 통신을 하지 않고 http(80)를 통해 통신하여 개인정보가 평문으로 전송되고 있음

로그인 페이지 암호화 전송	
회원관리 화면 평문 전송	POST [redacted] proc.php HTTP/1.1 Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */* Referer: [redacted] Accept-Language: ko-KR User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3) Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate Host: [redacted] Content-Length: 364 Connection: Keep-Alive Cache-Control: no-cache Cookie: hwaunique=1; hwatime=1397010625425; PHPSESSID=fee0d47460ee5ac28f526d9265d39df9 type=insert&findit=1&tid=1&bid=1&aid=1&comu_id=anjongik&comu_name=%BE%C8%C1%BE%C0%CD&comu_ssn1=850413&comu_ssn2=1[redacted]&comu_jisa=0&comu_bunryu=10&comu_pwd=4[redacted]&comu_pwd2=4[redacted]&comu_phone=028882222&comu_hp1=010&comu_hp2=8888&comu_hp3=8888&comu_addr_no1=151&comu_addr_no2=868&comu_addr1=%BC%AD%BF%EF+%B0%FC%BE%C7%B1%B8+%BD%C5%B8%B21%B5%BF+&comu_addr2=1461-22HTTP/1.1 200 OK Date: Wed, 09 Apr 2014 02:36:10 GMT Server: Hanbiro Server Centre(Powered by NetBSD) X-Powered-By: PHP/4.4.9 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Connection: close Transfer-Encoding: chunked Content-Type: text/html

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제23조(민감정보의 처리 제한) 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.

제24조(고유식별정보의 처리 제한) 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.

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.

【개인정보 보호법 시행령】

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

제30조(개인정보의 안전성 확보조치) 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 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제7조 개인정보의 암호화
- 개인정보 암호화 조치 안내서(2017, 행정안전부)
- 보안서버구축 안내서(2009, KISA)

4 접속기록의 보관 및 점검

세부분야	접속기록 보관				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.4.1	● **개인정보처리시스템의 접속기록을 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보처리시스템에 대한 로그파일은 기록하고 있으나 개인정보 처리 내역에 관한 사항으로 내용이 적절하지 않는 경우				
평가근거 및 의견	● ○○시스템은 웹 서버 로그 및 DB접근로그는 기록하고 있으나, 개인정보 처리 내역(조회, 출력, 다운로드 등)에 대한 로그는 기록되고 있지 않음				

주요 점검 사항

1. 개인정보취급자가 개인정보처리시스템에 접속한 기록은 1년 이상 보관·관리하여야 한다.
   ※ 개인정보처리시스템 접속 경로별로 누락없이 적용 필요(응용프로그램, DBMS, 서버 등)
2. 개인정보 접속기록은 아래 사항이 모두 포함되어 있어야 한다.
   ① 식별자
   ② 접속일시
   ③ 접속자를 알 수 있는 정보
   ④ 처리한 정보주체 정보
   ※ 검색조건문(쿼리)을 통해 대량의 개인정보를 처리한 경우 검색조건문을 정보주체 정보로 기록할 수 있으나, 해당시점의 DB를 백업하는 등 책임추적성 확보를 위해 필요한 조치를 하여야 함
   ⑤ 수행 업무(열람, 수정, 삭제, 인쇄, 입력, 다운로드 등)
   ※ 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등이 수행업무에 해당될 수 있음
   ※ 단, 주민등록번호, 계좌번호 등 민감한 개인정보가 포함되지 않도록 주의

지표 해설

● 개인정보처리시스템에 대한 개인정보담당자 등의 접속기록은 개인정보의 입·출력 및 수정사항, 파일별·담당자별 데이터접근내역 등을 자동으로 기록하는 로그 파일을 생성하는 불법적인 접근 또는 행동을 확인할 수 있는 중요한 자료이다. 따라서 「개인정보의 안전성 확보조치 기준 고시」에서는 접속기록을 1년 이상 의무적으로 보관하도록 규정하고 있다.

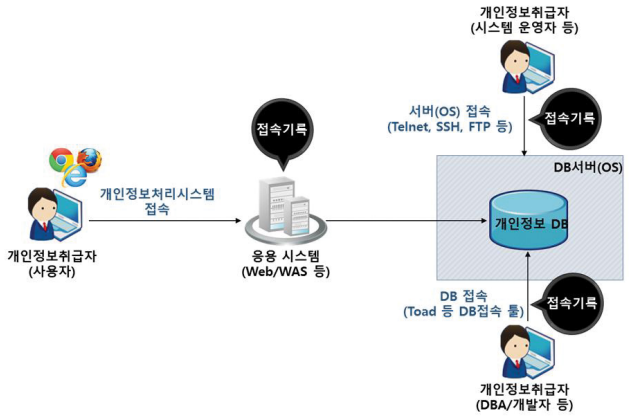
- ‘접속기록’이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 즉 ‘접속기록’에는 ①식별자, ②접속일시, ③접속자를 알 수 있는 정보, ④수행업무의 4가지 항목은 반드시 포함되어야 한다.

접속기록 항목 예시

No	필수 기록 항목	항목 예시	설명
①	식별자	ID	- 개인정보취급자 식별정보 - 사용자 계정, 사용자명 등
②	접속일시	날짜 및 시간	- 접속한 시점 또는 업무를 수행한 시점 (년-월-일, 시:분:초) - 시각동기화 등을 통해 정확한 시간 기록 필요
③	접속자를 알 수 있는 정보	접속자 IP 주소	- 접속한 자의 PC 또는 서버의 IP 주소
④	처리한 정보주체 정보	ID, 고객번호, 학번, 사번 등	- 개인정보취급자가 누구의 개인정보를 처리하였는지 알 수 있는 식별정보
⑤	수행업무	수행업무	- 개인정보에 대한 열람, 수정, 삭제, 인쇄, 입력, 다운로드 등 어떤 행위를 수행했는지 알 수 있는 구체적인 정보

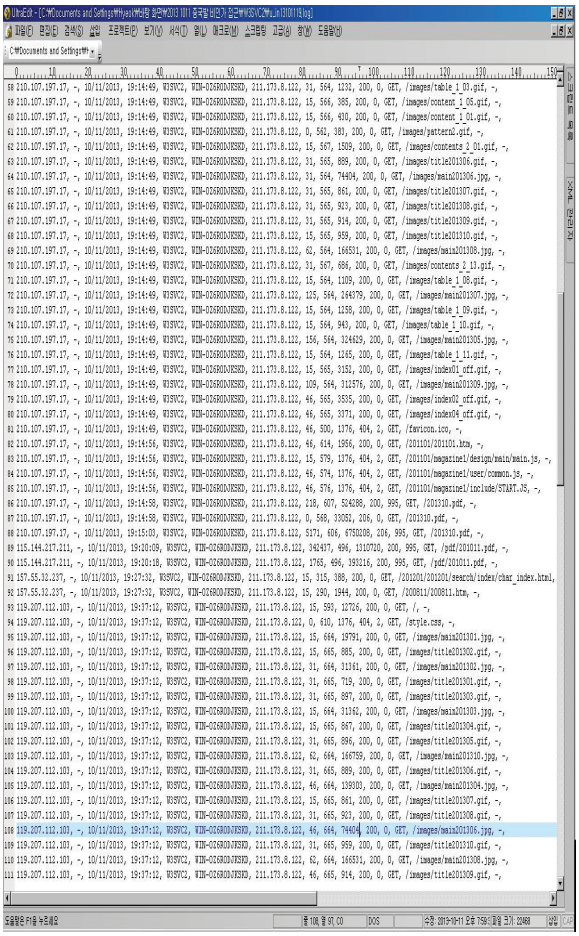
- 개인정보취급자가 개인정보처리시스템에 접속하는 경로 및 방법이 다양할 경우, 각각의 방법 및 경로별로 접속기록이 빠짐없이 기록될 수 있도록 하여야 한다.

개인정보처리시스템 접속 경로 예시



평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.4.1	개인정보처리시스템의 접속기록을 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○시스템은 웹서버 로그 및 DB접근로그를 통해 접속일시, 접속지 정보 등은 기록·관리하고 있으나, 수행업무(조회, 출력, 삭제, 다운로드 등)에 대한 로그는 기록되고 있지 않음 웹서버 로그				



관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리 시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제8조 접속기록의 보관 및 점검

세부분야	접속기록 점검				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.4.2	● **개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 정기적으로 점검하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보처리시스템에 대한 접속기록 점검 내역으로 단순한 로그 점검만으로 작성되어 있는 경우				
평가근거 및 의견	● ○○기관은 ○○시스템에 대하여 반기별 1회로 접속기록에 대한 점검을 수행하고 있으나, 점검결과를 살펴본 결과 일반적인 로그점검을 수행하였고, 과도한 조회, 대량 다운로드, 비업무 시간 접근 등에 대한 개인정보취급자의 수행업무를 분석한 구체적인 내용은 반영되어 있지 않음				

주요 점검 사항

1. 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 점검계획을 수립하고, 그 계획에 따라 월 1회 이상 점검하여야 한다.
   ※ 점검계획에는 점검 방법, 점검 기준, 점검 주기/시점, 담당자, 비정상 행위 발견 시 대응 절차, 보고 절차 등 포함 필요
2. 대량 개인정보 다운로드, 과도한 개인정보 조회 등 위험 행위를 효과적으로 점검할 수 있도록 기술적인 방안이 마련되어야 한다.
   ※ 응용프로그램 기능 구현, 로그분석시스템 도입 등

지표 해설

- 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보 처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.
  이를 통해 비인가된 개인정보 처리, 대량의 개인정보의 조회, 정정, 다운로드, 삭제 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있다.

- 접속기록의 효과적인 점검이 가능하기 위해서는 접속기록 점검 계획의 수립, 검색기능 구현 등 관리적, 기술적 방안이 함께 마련될 필요가 있다.

접속기록 점검 방안 예시	
항목	설 명
접속기록 점검계획 (관리적 방안)	- 점검 방법/담당자 : 수작업 또는 자동화 도구 활동 등 - 점검 기준 : 유명인사 조회, 짧은 시간 내 대량 조회·다운로드, 야간 또는 주말 접속, 특정 건수 이상의 과다 조회, 민감정보 조회 등 - 점검 주기 : 일 단위/월 단위/분기 단위/반기 단위 등 - 보고 절차 : 점검결과 보고 절차, 의심사항 발견 시 조치 방법 및 절차 등
점검기능 구현 (기술적 방안)	- 점검계획에서 수립된 점검방법, 점검기준, 점검주기 등을 효과적이고 효율적으로 수행할 수 있도록 기능 구현 · 개인정보처리시스템의 응용프로그램 기능으로 구현(검색기능 등) · DB접근제어 등 보안시스템에서 제공하는 기능 활용 · 별도의 통합로그분석시스템 도입 및 적용 등 ※ 일반적으로 '접속기록'의 Size가 매우 크기 때문에 수작업 점검을 통해 비정상 이벤트를 찾아내는 것은 쉽지 않으므로, 가급적 기술적인 기능으로 구현할 것을 권고함

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.4.2	개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 정기적으로 점검하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○기관은 ○○시스템에 대하여 월 1회로 접속기록에 대한 점검을 수행하고 있으나, 점검결과를 살펴본 결과 일반적인 로그점검을 수행하였고, 과도한 조회, 대량 다운로드, 비업무 시간 접근 등에 대한 개인정보취급자의 수행업무를 분석한 구체적인 내용은 반영되어 있지 않음 접속기록 점검 증적 				

접속기록 점검 증적	LOG 분석표

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제8조(접속기록의 보관 및 점검)

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제8조 접속기록의 보관 및 점검

세부분야	접속기록 보관 및 백업				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.4.3	● 개인정보처리시스템의 접속한 기록을 최소 6개월 이상 보관하고 위변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관하도록 계획되고 있습니까?		○		
평가 예시	● 부분이행 : 개인정보DB 접근 및 이용로그를 백업하여 관리하고 있으나, 별도 저장장치에 백업하여 관리되고 있지 않는 경우				
평가근거 및 의견	● ○○시스템에 대한 DB로그 및 시스템 로그 등을 정기적(1개월)으로 백업하여 저장하고 있으나, ○○시스템 디렉터리에 백업파일을 보관하고 있음				

주요 점검 사항

1. 개인정보처리시스템의 접속기록이 위·변조 및 도난, 분실 되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
   ① 정기적으로 접속기록 백업 수행 및 별도의 저장장치에 보관
   ② 덮어쓰기 방지 매체 사용
   ③ 기타 접속기록의 무결성을 보장할 수 있는 기술적·관리적 방안 적용 등의 방법 활용

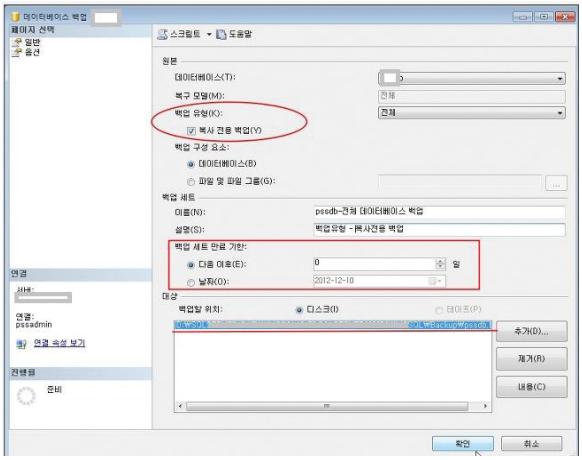
지표 해설

- 개인정보처리자는 개인정보처리시스템의 접속 기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.

- 안전하게 보관하는 방법으로는 여러 가지 방법들이 존재하며, 이러한 방법들 중에 대상기관에 맞는 방법을 선택하여 사용할 수 있다. 다만 개인정보처리시스템과 동일한 서버에 접속기록이 존재하게 될 경우에는 위·변조, 도난, 분실 등을 방지하는 것이 어려우므로 최소한 물리적으로 분리된 저장장치에 보관·백업될 수 있도록 하여야 한다.

  - 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하는 등의 조치 필요
  - 접속기록에 대한 위·변조를 방지하기 위해서는 CD-ROM, WORM(Write Once Read Many) 등과 같은 덮어쓰기 방지 매체를 사용하는 것을 권고함
  - 접속기록을 수정 가능한 매체(하드디스크, 자기테이프 등)에 백업하는 경우 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음
    (예를 들어, 접속기록을 HDD에 보관하고 위·변조 여부를 확인할 수 있는 정보(MAC값, 전자서명값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리할 수 있음)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.4.3	개인정보처리시스템의 접속한 기록을 최소 6개월 이상 보관하고 위변조 및 도난, 분실되지 않도록 별도 저장 장치 등에 백업 보관하도록 계획되고 있습니까?		○		
평가근거 및 의견	● ○○시스템에 대한 DB로그 및 시스템 로그 등을 정기적(1개월 단위)으로 백업하여 저장하고 있으나, ○○시스템 로컬 디렉터리에 백업파일을 보관하고 있음 로컬 DB 백업 				

관련법령 및 문서

관련 법령 · 지침

【개인정보의 안전성 확보조치 기준 고시】

제8조(접속기록의 보관 및 점검) ③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제8조 접속기록의 보관 및 점검

5 악성프로그램 등 방지

세부분야	백신 설치 및 운영				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.5.1	● **개인정보처리단말기에 악성프로그램을 점검, 치료할 수 있는 백신프로그램을 설치하고 최신업데이트 및 악성프로그램의 주기적 점검 등 대응조치를 실시하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보를 처리하는 단말기에 백신프로그램을 설치되어 있으나 최신 업데이트 관리가 안되는 경우				
평가근거 및 의견	● 업무용 단말기(PC)에 백신프로그램이 설치되어 운영되고 있으나, 백신 자동업데이트가 되어 있지 않아 최신 업데이트 관리가 되지				

주요 점검 사항

1. 악성프로그램 등을 방지·치료할 수 있는 백신소프트웨어 등의 보안프로그램을 설치·운영하여야 한다.
   ※ 개인정보처리시스템(윈도우 기반), 개인정보취급자 PC 등
   ① 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
   ② 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
   ③ 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

지표 해설

- 악성 프로그램은 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.
- 개인정보처리자는 악성 프로그램 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치·운영하여야 한다. 이러한 백신 소프트웨어는 개인정보취급자 PC 뿐만 아니라, 윈도우즈 기반의 개인정보처리시스템에도 설치·운영할 필요가 있다.
- 백신 소프트웨어 등의 보안 프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지하여야 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 유지하여야 하며, 백신 소프트웨어 등에서 제공하는 자동 업데이트 기능 등을 활용하면 편리하고 신속하게 조치할 수 있다.

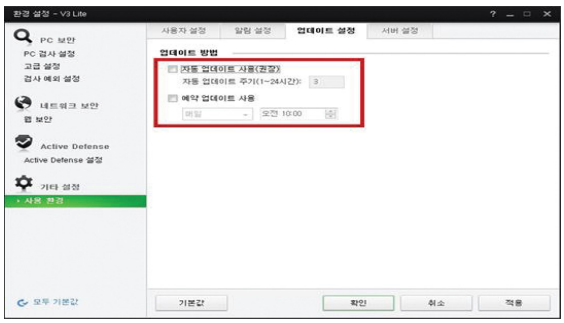
- 특히 대량의 개인정보를 처리하거나 민감한 정보 등 중요도가 높은 개인정보를 처리하는 경우에는 키보드, 화면, 메모리해킹 등 신종 악성프로그램에 대해 대응할 수 있도록 보안프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지해야 한다.

● 외부에서 개인정보처리시스템에 접속하여 개인정보를 취급하는 운영 위탁 등 외부 인력의 단말에서 개인정보처리시스템에 접속할 경우에는 개인정보처리시스템 이용 시 백신 소프트웨어 설치·운영이 의무사항임을 안내창 또는 공지사항 등을 이용하여 주기적으로 안내하는 기능을 구현 할 수 있다.

백신 소프트 웨어 설정 예시

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.5.1	개인정보처리단말기에 악성프로그램을 점검, 치료할 수 있는 백신프로그램을 설치하고 최신업데이트 및 악성프로그램의 주기적 점검 등 대응조치를 실시하도록 계획하고 있습니까?		○		
평가근거 및 의견	● 업무용 단말기(PC) 및 윈도우 서버에 V3 백신프로그램이 설치되어 운영되고 있으나, 자동업데이트 기능 비활성화로 인하여 백신프로그램이 최신 업데이트 관리가 되지 않음 백신 프로그램이 자동 업데이트 되지 않음				



관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

5. 개인정보에 대한 보안프로그램의 설치 및 갱신

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제9조(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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제9조 악성프로그램 등 방지

세부분야	보안 업데이트 적용				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.5.2	● **악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램, 운영체제 소프트웨어 제작업체에서 보안 업데이트 공지가 있는 경우, 이에 따른 업데이트가 지체 없이 실시되도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 운영체제에 대해 최신 보안업데이트를 적용하였으나, 일부 누락된 운영체제나 응용프로그램이 있는 경우				
평가근거 및 의견	● 패치관리시스템을 도입하여 윈도우 계열의 서버 및 PC에 대해서는 보안 업데이트를 관리하고 있으나, 리눅스 운영체제를 사용하는 ○○○서버에 대해서는 최신 보안업데이트가 적용되지 않음				

주요 점검 사항

1. 운영체제(OS), 응용프로그램 등의 보안취약점을 악용하는 악성프로그램 관련 경보가 발령되거나, 해당 제작업체에서 보안 업데이트 공지가 있는 경우 지체 없이 이에 따른 업데이트를 실시하여야 한다.
2. 윈도우 2003서버, 윈도우XP 등 해당 제작업체에서 기술 지원이 종료된 운영체제는 업그레이드 계획을 수립·이행하여야 한다.
3. 운영 중인 개인정보처리시스템에 보안 업데이트를 적용하는 경우에는 사전에 영향도를 분석 후 적용하여야 하며, 불가피한 사유로 보안 업데이트 적용이 어려운 경우 이에 따른 보완대책이 적용되어야 한다.

지표 해설

● 운영체제(OS)·응용 프로그램의 보안 취약점을 악용하는 악성 프로그램 경보가 발령되었거나, 응용 프로그램, 운영체제 제작업체에서 보안 업데이트(패치 등) 공지가 있는 경우에는 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 즉시 업데이트를 실시하여야 한다.

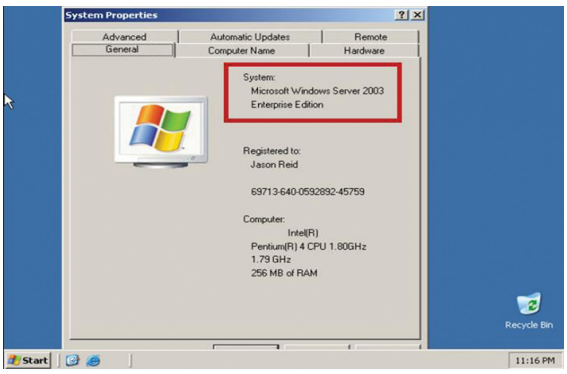
- 운영체제나 응용 프로그램 보안 업데이트 시 현재 운영 중인 응용 프로그램의 업무 연속성이 이루어 질 수 있도록 보안 업데이트를 적용하는 것이 필요하며, 가능한 자동으로 보안 업데이트가 설정되도록 할 필요가 있다.
- 적용 대상 예시 : OS(윈도우, 유닉스, 리눅스), 상용 또는 공개S/W(Oracle, MySQL, OpenSSL, Apache, IIS 등), 보안 및 네트워크 장비(Cisco 등) 등

● 윈도우 2003서버, 윈도우 XP 등 해당 제작업체에서 기술지원이 종료된 운영체제는 더 이상 보안 업데이트가 배포되지 않기 때문에 새로운 취약점이 발견되어도 대응이 어렵다. 따라서 기술지원이 종료된 운영체제, 응용 프로그램은 최신 버전으로 전환하여 최신 보안업데이트를 지속적으로 적용할 수 있도록 하여야 한다.

- 운영 중인 시스템에 보안 업데이트를 적용하는 경우 충돌이나 장애 등 시스템 가용성에 영향을 미칠 수 있으므로, 운영시스템의 중요도와 특성을 고려하여 내부 절차에 따라 충분하게 영향을 분석한 후 적용할 필요가 있다. 다만, 운영 환경에 따라 즉시 보안업데이트가 어려운 경우 그 사유와 추가적인 보완대책을 마련하여 책임자에게 보고하고 그 현황을 관리하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.5.2	악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램, 운영체제 소프트웨어 제작업체에서 보안 업데이트 공지가 있는 경우, 이에 따른 업데이트가 지체 없이 실시되도록 계획하고 있습니까?		○		
평가근거 및 의견	● 윈도우 계열의 서버 및 PC는 패치관리시스템(APC)를 통해 최신 보안업데이트 관리를 하고 있으나, 백업 용도로 사용하고 있는 ○○○서버의 OS는 2015년에 기술지원이 종료된 윈도우2003서버를 사용하고 있으며, 별도의 보완대책이 수립되어 있지 않음				

취약한 운영체제 사용 (OOO 서버)	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

5. 개인정보에 대한 보안프로그램의 설치 및 갱신

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제9조(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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제9조 악성프로그램 등 방지

6 물리적 접근방지

세부분야	출입통제 절차 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.6.1	● **전산실, 자료보관실 등 개인정보를 보관하는 물리적 장소에 대한 출입통제 절차를 수립·운영하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 출입통제 장치는 설치되어 있으나, 출입통제 절차가 미흡하거나 일부 불필요한 인원이 출입자로 등록되어 있는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 전산실에 CCTV와 지문을 이용한 출입통제장치가 설치되어 비인가자의 출입을 통제하고 있으나 출입권한에 정기적인 검토가 부재하고 최근 퇴직한 인원(홍** 등)이 출입자로 등록되어 있음				

주요 점검 사항

1. 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
   ① 출입통제 절차 수립(출입자 등록·삭제, 출입권한 검토, 출입기록 검토, 방문자 관리 등)
   ② 물리적 접근방지를 위한 출입통제 장치 설치(비밀번호 기반, 카드기반, 생체정보 기반 등)
   ③ 출입내역을 전자적 매체 또는 수기문서 대장에 기록 등

지표 해설

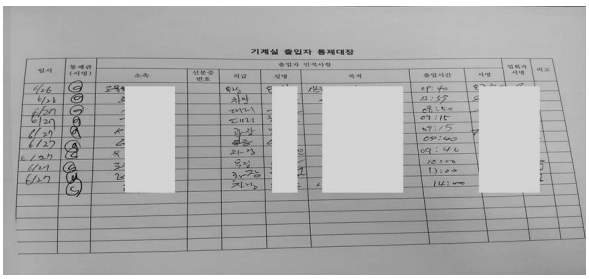
- 개인정보를 대량으로 보관하고 있는 전산실·자료보관실 등 물리적 보관장소를 별도로 두고 있는 경우, 출입자에 의한 개인정보 대량 유출의 위험이 있으므로 이에 대한 출입통제 절차를 수립하여 운영하는 등 보안대책을 마련하여 대응할 필요가 있다.
- 개인정보를 대량으로 보관하고 있는 전산실·자료보관실을 별도로 두고 있는 경우에는 비인가자의 출입에 의한 개인정보가 포함된 정보자산의 절도, 파괴 등 물리적 위협에 대응하기 위해 출입통제 절차를 수립·운영하여야 한다.
  - 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적 공간으로 전기시설, 공조시설, 소방시설 등을 갖춘 시설을 의미함
  - 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 장소를 의미함

- 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 접근방지를 위한 장치(예시) : 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입통제 장치, 지문 등 바이오정보 기반 출입통제 장치 등

- 전산실·자료보관실 등에 대하여 인가된 사람만이 출입할 수 있도록 하고 사고 발생을 대비한 책임추적성을 확보하기 위해서는 출입통제 시스템의 설치와 더불어 이를 제대로 관리할 수 있는 효과적인 출입통제 절차의 수립이 필요하다. 출입통제 절차를 수립할 때에는 아래의 사항을 고려할 수 있다.

출입통제 절차 수립 시 고려사항
- 출입권한 등록·변경·삭제 절차 : 출입권한 신청 및 승인 절차, 퇴직 절차 등 - 출입자 관리 : 출입자 목록 등을 통한 출입자 현황 관리 등 - 출입권한 및 이력 검토 절차 : 출입권한 및 출입기록의 적정성 검토 방안(검토 주기, 담당자 등) - 방문자 관리 : 출입 신청 및 승인, 방문증 발급·회수, 에스코트, 출입 대장 기록 등 - 기타 사항 : 출입통제 시스템 현황, 정기 점검 등 ※ 업무 목적에 따라 최소한의 인원만이 출입할 수 있도록 하여야 함

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.6.1	전산실, 자료보관실 등 개인정보를 보관하는 물리적 장소에 대한 출입통제 절차를 수립·운영하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 전산실 출입자에 대해 '출입대장'을 기재하여 관리하고 있음. 하지만 '회의록_2014XXXX'에 2014년 4X월XX일 유지보수 업체 직원이 전산실에 방문한 것으로 확인되나(김○○) 출입대장에 기재하지 않았음. 전산실 출입대장 				

회의록	회 의 록 목 적: 2014년 일 시: 2014년 장 소: 회의실 참석자(5인): 문 회 의 내 용 □ 회의 내용 1. : o - o 4/14일 서버 유지보수 업체 방문 전산실 서버 점검 - 김 ! 대리 (30분 작업) => 이상 없음

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제11조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제11조 물리적 안전조치

세부분야	반출·입 통제 절차 수립				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.6.2	● **개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 보조저장매체 반·출입 통제절차가 수립되어 시행되고 있으나, 보조저장매체의 현황 관리가 미흡한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '보조저장매체 반·출입 통제절차'를 마련하여 시행하고 있으나, ○○부서에서 개인정보 취급 목적으로 사용 중인 보조저장매체는 관리대장에 등록되어 있지 않음				

주요 점검 사항

1. 개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관하여야 한다.
   ※ 잠금 상태에 대한 관리·감독 필요
2. 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.
   ① 보조저장매체 현황 관리
   ② 보조저장매체 반출·입 절차 및 대장 관리 등

지표 해설

- 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체(USB, CD 등) 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
  - 플로피디스켓, 이동형 하드디스크, USB메모리, SSD, CD, DVD 등의 보조기억매체는 금고 또는 잠금장치가 캐비넷 등에 안전하게 보관하여야 한다.

- 개인정보처리시스템을 운영하는 개인정보처리자는 USB메모리, 이동형 하드디스크 등의 보조저장 매체를 통해 개인정보가 유출되지 않도록 개인정보가 저장·전송되는 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.
  - 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 보조저장매체 반출·입 통제를 위한 보안대책 마련이 필수는 아니나, 관련 대책 마련을 권장한다.

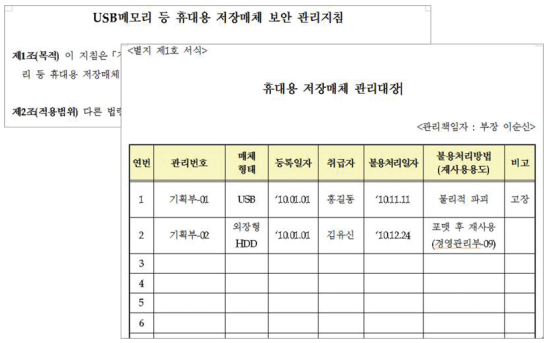
보조저장매체의 반출·입 통제를 위한 보안대책 마련 시 고려사항
- 보조저장매체 보유 현황 파악 및 반출·입 관리 계획 - 개인정보취급자 및 수탁자 등에 의한 개인정보 유출 가능성 - 보조저장매체의 안전한 사용 방법 및 비인가된 사용에 대한 대응 - USB를 PC에 연결시 바이러스 점검 디폴트로 설정 등 기술적 안전조치 방안 등

● 보조저장매체 반·출입 통제를 위한 보안대책은 전사적으로 수집되어 운영되도록 할 필요가 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.6.2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 '휴대용 저장매체 보안관리지침'을 수립하였으며, 해당 지침에 따라 휴대용 저장매체 관리를 시행하고 있음. 하지만, '휴대용 저장매체 관리지침'에 민원실에서 개인정보 전달 목적으로 구입한 USB 메모리 2개가 목록에서 누락되어 있음				

휴대용 저장매체 관리지침 및 관리대장	



USB메모리 등 휴대용 저장매체 보안 관리지침

제1조(목적) 이 지침은 「

리 등 휴대용 저장매체

제2조(적용범위) 다른 법

<별지 제1호 서식>

휴대용 저장매체 관리대장

<관리책임자 : 부장 이순신>

연번	관리번호	매체 형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용용도)	비고
1	기획부-01	USB	'10.01.01	홍길동	'10.11.11	물리적 파괴	고장
2	기획부-02	외장형 HDD	'10.01.01	김유신	'10.12.24	포맷 후 재사용 (경영관리부-09)	
3							
4							
5							
6							

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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.

【개인정보 보호법 시행령】

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

6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제11조(물리적 안전조치)

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제4장 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 해설서 – 제11조 물리적 안전조치

7 개인정보의 파기

세부분야	안전한 파기				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.7.1	● **개인정보를 파기할 경우 복구 또는 재생되지 않는 방법으로 파기하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 개인정보의 완전 삭제를 위한 절차, 방법 등이 도입되어 있으나, 일부 누락되는 경우가 존재하는 경우				
평가근거 및 의견	● ○○시스템 내 보유하고 있는 개인정보파일에 대한 파기수행 시 개인정보 보호지침에 파기절차 및 방법은 명시되어 있으나 개인정보 파기 시 파기 솔루션 등을 통해 복구 또는 재생되지 않는 방법으로 파기가 되고 있지 않음				

주요 점검 사항

1. 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 안전하게 파기하여야 한다.
   ① 완전파괴(소각·파쇄 등)
   ② 전용 소자장비를 이용하여 삭제
   ③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행(완전삭제 프로그램 등)
2. 개인정보의 일부만을 파기하는 경우 등 기술적으로 안전한 파기가 어려운 경우에는 아래와 같이 복구 또는 재생의 위험을 최소화할 수 있는 방법을 적용하여야 한다.
   ① 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리·감독
   ② 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제
3. 개인정보처리시스템 및 개인정보취급자 단말기의 저장매체를 교체 또는 폐기하는 경우 내부 개인정보 데이터가 복구 또는 재생되지 않도록 조치를 취하여야 한다.

지표 해설

- 개인정보처리자는 개인정보 수집목적 달성, 보존기간의 경과 등 개인정보가 불필요하게 되었을 때에는 개인정보의 유출 및 오남용 방지를 위해 개인정보를 복원이 불가능한 방법으로 파기가 필요하다. 또한, 개인정보 파기 방법 중 개인정보의 일부만 파기시 완전파괴 방법 등을 사용하지 어려운 특정 환경에서도 복구 및 재생되지 않도록 조치하는 방법이 필요하다.
- 개인정보를 복구 또는 재생되지 아니하도록 파기할 때에는 개인정보가 저장된 매체에 따라 아래와 같은 방법을 사용할 수 있다.

개인정보를 안전하게 파기할 수 있는 방법 예시	
파기 방법	예 시
완전파괴(소각·파쇄 등)	- 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기하거나 용해 또는 소각장, 소각로에서 태워서 파기 등
전용 소자장비를 이용하여 삭제	- 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 등
데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행	- 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

- 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 파기에 관한 사항을 기록·관리하여야 한다.

- "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·감독
  - 전자적 파일 외의 기록물, 인쇄물, 서면 등 : 해당 부분을 마스킹, 천공 등으로 삭제

- 개인정보처리시스템 및 개인정보취급자 단말기(PC 등)의 스토리지, HDD, 테잎 등 저장매체를 교체, 재사용, 폐기하는 경우에는 매체에 기록된 개인정보가 복구 불가능하도록 완전히 삭제하여야 한다.

- 개인정보처리자는 복원이 불가능한 방법으로 개인정보를 파기하여야 하는데, 예를 들어 전자기적으로 기록된 개인정보는 비록 삭제하였다고 하더라도 복원기술을 적용할 경우에는 그 정보가 복구될 가능성도 있다. 따라서 말 그대로 '복원이 불가능한 방법'을 적용하기 위해서는 상당한 비용이 소요될 수도 있다. 이를 위하여 표준지침은 '복원이 불가능한 방법'이란 사회 통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 말하고 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.7.1	개인정보를 파기할 경우 복구 또는 재생되지 않는 방법으로 파기하도록 계획하고 있습니까?		○		
평가근거 및 의견	● ○○시스템 내 보유하고 있는 개인정보파일에 대한 파기수행 시 개인정보보호지침에 파기절차 및 방법은 명시되어 있으나 개인정보 파기 시 파기 솔루션 등을 통해 복구 또는 재생되지 않는 방법으로 파기가 되고 있지 않음				

개인정보 보호지침 내 개인정보 파기 방법 및 절차	**제17조(개인정보의 파기방법 및 절차)** ① 개인정보처리자는 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정한 날로부터 5일 이내에 그 개인정보를 파기하여야 한다. ② 개인정보를 파기할 경우 다음 각 호의 구분에 따른 방법으로 하여야 한다. 1. 전자적 파일 형태인 경우 : 복원이 불가능한 방법으로 영구 삭제 2. 제1호 이외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각 ③ 개인정보의 파기에 관한 사항을 기록 · 관리하여야 한다. ④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다. ⑤ 개인정보처리자는 개인정보파일 파기에 관하여는 제59조 및 제60조를 적용한다. ⑥ 분야별 책임자는 개인정보의 파기에 관한 사항을 별표 5(개인정보파일 파기관리대장)로 기록 · 관리한다.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제21조(개인정보의 파기) ② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

【개인정보 보호법 시행령】

제16조(개인정보의 파기방법) 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 보호위원회가 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제13조(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, 서명, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

【표준 개인정보 보호지침】

제10조(개인정보의 파기방법 및 절차)

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.

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.

관련 문서

- 인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제21조
- 개인정보의 안전성 확보조치 기준 해설서 – 제13조 개인정보의 파기

8 기타 기술적 보호조치

세부분야	개발 환경 통제				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.8.1	● 개발환경을 통한 개인정보의 유출을 방지하기 위하여 테스트 데이터 생성·이용·파기 및 기술적 보호조치 등에 관한 대책을 적용하도록 계획하고 있습니까?			○	
평가 예시	● 미이행 : 프로그램 테스트 데이터에 개인정보를 포함하여 테스트를 마친 후 개인정보가 제거되지 않은 경우				
평가근거 및 의견	● 기존 운영시스템 DB에서 개발서버 DB로 개인정보를 가져와 일부 항목만 수정하여 가공 개인정보 데이터로 변환하여 테스트를 수행한 이후 가공 개인정보 데이터를 삭제하지 않고 있음				

주요 점검 사항

1. 개인정보처리시스템의 개발 및 시험환경에서 사용되는 테스트 데이터는 실제 운용되는 개인정보가 아닌 가공된 정보로 변환하여 사용하여야 한다.
2. 불가피하게 실제 운용되는 개인정보를 테스트 데이터로 사용하여야 하는 경우에는 개인정보의 사용범위를 제한하고 개인정보처리시스템과 동일한 수준의 보호조치를 적용하여야 하며, 테스트 종료 등 테스트 데이터 사용이 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기하여야 한다.
3. 개인정보처리시스템의 운영환경과 개발환경은 원칙적으로 분리하여야 하며, 개발환경에서 운영환경으로의 접속 및 이관은 통제된 절차에 따라 수행되어야 한다.
4. 개인정보처리시스템의 소스프로그램에 대한 비인가자의 접근을 차단하는 등 소스프로그램에 대한 악의적인 변경 및 유출에 대한 보호대책을 적용하여야 한다.

지표 해설

- 테스트 데이터에는 실제 운용되는 개인정보가 아닌 가공된 형태의 정보로 테스트를 실시하도록 권장한다.
- 불가피하게 실제 운용하고 있는 개인정보를 테스트 데이터로 활용하는 경우에는 개인정보의 사용 범위를 제한하고 개인정보처리시스템과 동일한 수준으로 안전성 확보조치를 적용하여야 한다. 또한 테스트 종료 등으로 해당 데이터가 불필요하게 되었을 때는 지체 없이 파기하도록 하여야 한다.
  ※ 개발시스템에서 실제 개인정보를 보유하는 경우, 해당 개발시스템도 「개인정보 보호법」 상의 개인정보처리시스템에 해당될 수 있음

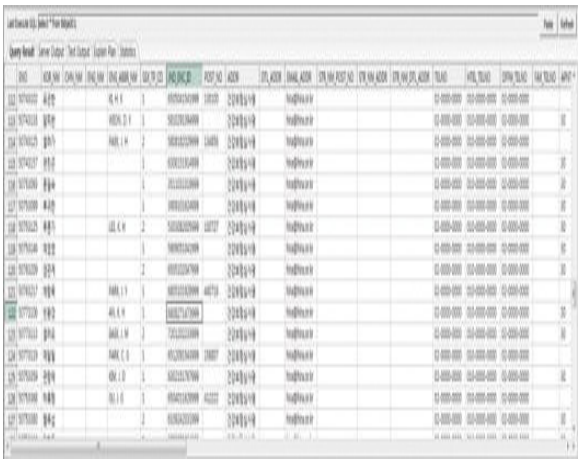
- 개발환경에서 운영환경은 원칙적으로 분리되어야 하며 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 한다. 이를 위해 운영환경으로의 이관 절차를 수립·이행할 것을 권장한다.
  - 이관 담당자 및 책임자
  - 이관 기준 및 절차(승인 절차, 시험방안 등)
  - 문제 발생 시 조치방안 등

- 불가피하게 개발환경과 운영환경 분리가 어려운 경우, 운영환경에 대한 비인가자의 접근 및 변경의 위험을 감소시키기 위하여 변경사항의 검토 및 승인, 작업자의 책임추적성 확보 등 보완통제를 마련할 필요가 있다.

- 개인정보처리시스템의 소스프로그램의 유출 및 불법 변경 등을 방지하기 위하여 접근 통제, 변경 관리 등 소스프로그램에 대한 보안 통제를 적용할 것을 권장한다.
  - 소스프로그램에 대한 변경 이력 관리
  - 소스프로그램 백업
  - 비인가자의 소스프로그램 접근을 통제하기 위한 절차 수립·이행 (실제 운영환경에는 소스프로그램을 보관하지 않도록 주의)

    ※ 형상관리 소프트웨어를 이용할 경우 효과적으로 통제 가능함

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.8.1	개발환경을 통한 개인정보의 유출을 방지하기 위하여 테스트 데이터 생성·이용·파기 및 기술적 보호조치 등에 관한 대책을 적용하도록 계획하고 있습니까?			○	
평가근거 및 의견	● 기존운영시스템 DB에서 고도화 사업을 위해 개발서버 DB로 개인정보를 가져와 프로그램 동작여부를 테스트 하고자 할 때, 기존 DB정보에서 다른 필드는 그대로 실 데이터를 유지하고, 이름정보만 가공데이터로 변환하여 테스트를 수행하고 있으며,테스트 완료 후 가공된 테스트 데이터를 즉시 삭제하지 않고 일정기간 보관되고 있음 테스트 데이터 				

관련법령 및 문서

관련 법령 · 지침

● 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

세부분야	개인정보 처리화면 보안				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.8.2	● **개인정보취급자 및 정보주체의 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹 브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 카드번호 등 중요정보에 대한 복사·화면캡쳐 방지 및 키보드해킹 방지 등 보호대책을 적용하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 중요 개인정보의 특정자릿수를 별표(*)등의 임의문자로 치환하도록 화면설계서 등의 설계문서에서 확인할 수 없는 경우				
평가근거 및 의견	● ○○시스템의 회원가입 시 본인확인 과정에서 고유식별정보를 입력하는 경우 특정 자릿수에 대하여 임의문자 치환 없이 고유식별정보를 그대로 노출하고 있음				

주요 점검 사항

1. 개인정보취급자 및 정보주체의 단말기에서 개인정보 처리 화면 등을 통한 개인정보의 유·노출을 방지하기 위하여 보호대책이 적용되어야 한다.
   ① 용도에 다른 개인정보 표시항목 최소화
   ② 개인정보 표시제한 보호조치(마스킹)
   ③ 웹브라우저 우측 마우스버튼 제한(소스보기 등 제한)
   ④ 웹브라우저 히스토리 기능을 통한 개인정보 노출 통제(Back 버튼, URL 히스토리 등)
   ⑤ 개인정보가 포함된 임시파일 및 캐시 생성 통제 등
   ※ 개인정보 표시제한 보호조치 적용 시에는 일관성 있게 적용될 수 있도록 표준을 정의하여야 함
2. 카드번호, 계좌번호, 주민등록번호 등 중요 정보에 대해서는 처리화면 등을 통한 개인정보의 유·노출을 방지하기 위하여 강화된 보호조치 적용이 검토되어야 한다.
   ① 키보드 해킹 방지
   ② 화면캡쳐 및 복사 방지 등

지표 해설

● 개인정보취급자 및 정보주체가 개인정보처리시스템에 접속하여 개인정보를 입력, 조회, 변경, 삭제, 출력, 다운로드 등 처리하는 과정에서 단말기(업무용 컴퓨터 등), 웹브라우저 등 응용프로그램의 처리화면 등을 통해 개인정보가 불필요하게 노출되거나 유출되지 않도록 보호조치를 적용할 필요가 있다.

개인정보 처리단말기 및 처리화면을 통한 개인정보 유·노출 방지 조치		
No	항목	설명
①	용도에 따른 개인정보 처리항목 최소화	- 개인정보를 화면에 표시하거나 출력, 파일생성(다운로드) 하는 경우 용도를 특정하여야 하며 용도에 따라 개인정보 항목을 최소화하여야 함 - 예를 들어, 홈페이지 회원정보를 리스트로 보여주는 화면에서는 업무상 불필요한 상세 주소를 보여주지 않도록 조치 등
②	개인정보 표시제한 조치	- 개인정보를 화면 등에 표시할 때 해당 개인정보 항목 전체를 보여줄 필요가 없을 경우, 해당 개인정보의 일부분을 마스킹하여 전체정보가 불필요하게 노출되지 않도록 하여야 함 - 개인정보의 마스킹을 통해 표시제한 조치를 취하려는 경우에는 대상기관의 마스킹 적용규칙을 마련하여 개인정보처리시스템 및 처리화면별로 일관성을 가질 수 있도록 할 필요가 있음 - 웹 화면 상에서는 마스킹되었으나 소스프로그램 보기 시 전체 정보가 노출되는 경우가 있으므로 주의가 필요함
③	웹브라우저 우측마우스 버튼 제한	- 개인정보가 표시되는 웹브라우저 화면에서의 소스프로그램 보기, 텍스트 드래그 및 복사 등을 방지하기 위해서 우측마우스 버튼 제한 조치를 적용할 수 있음 - 우측 마우스 버튼 제한은 Javascript와 같은 스크립트를 적용하거나 웹DRM와 같은 보안기술을 적용할 수 있음 - 단, 스크립트 방식은 우회방법이 존재할 수 있으며, 경우에 따라 사용자 불편을 초래할 수 있으므로 대상 시스템 및 대상 화면별 특성에 따라 적용 방법 및 적용 여부를 선택할 수 있음
④	웹 브라우저 히스토리 통제	- 웹브라우저에 개인정보 처리화면 접속 히스토리가 남을 경우 이를 통해 제3자에게 개인정보가 노출될 위험성이 있음 - 비밀번호 등 개인정보는 "GET" 방식으로 전송하지 않도록 해야 함 (웹 브라우저의 주소창 히스토리에서 개인정보 노출 가능)
⑤	개인정보가 포함된 캐시 및 임시 파일 생성 통제	- 고유식별정보, 금융정보 등 민감한 개인정보를 표시하는 화면은 웹 브라우저의 뒤로 가기(Back) 버튼을 클릭해서 조회하면 기존 정보가 보이지 않도록 조치할 필요가 있음(No-Cache 설정 등) - 개인정보의 출력, 다운로드 등 처리과정에서 개인정보처리 단말기에 임시파일이 저장되지 않도록 조치해야 함 (불가피하게 생성되는 경우에는 처리 완료 후 완전 삭제 되도록 해야 함)

- 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 별표(*) 등 표시제한 조치를 취하는 경우에는 다음의 원칙으로 적용할 수 있다. (대상기관에 환경 등을 반영하여 자율적으로 결정)

· 성명 중 이름의 첫 번째 글자 이상
· 생년월일
· 전화번호 또는 휴대폰 전화번호의 국번
· 주소의 읍/면/동
· 인터넷주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

성명	홍*동	생년월일	****년 *월 *일
전화번호	02-****-1234	핸드폰	010-****-1234
주소	서울 종로구 ***동 12-3	접속지 IP	123.123.***.123

● 카드번호, 계좌번호, 주민등록번호, 민감정보 등 중요한 개인정보를 처리하는 경우에는 대해서는 보다 강화된 보호조치 적용이 권장된다.

개인정보 처리화면에 대한 강화된 보호조치		
No	항목	설명
①	키보드 해킹방지	- 키로거와 같은 악성코드 감염으로 인한 키보드 입력값 유출을 방지하기 위하여 개인정보취급자 또는 정보주체의 단말기(PC, 모바일 기기 등)에 키보드 해킹방지 솔루션을 적용할 필요가 있음 - 키보드 해킹방지를 적용할 경우 프로그램 설치 등 사용자 불편 등이 발생할 수 있으므로 사용자 편의성과 처리되는 정보의 중요성 및 유출 위험성 등을 고려하여 적용여부를 결정
②	화면 캡쳐 및 복사 방지	- 웹브라우저 등 개인정보 처리화면에 대한 화면 캡쳐 및 복사를 통하여 민감한 개인정보가 유출되는 것을 방지하기 위해서는 화면캡쳐 방지솔루션(웹DRM 등)의 도입을 고려할 수 있음 - 모든 화면에 적용하기 보다는 해당 화면이 캡쳐되어 유출될 경우 영향이 큰 경우에 한해 적용할 것을 권장함 - 단, 스마트폰으로 촬영하거나 수기로 옮겨 적는 방법으로도 유출이 가능하기 때문에 화면캡쳐방지 솔루션 도입의 효과성을 면밀히 검토하여 결정할 필요가 있음

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.8.2	개인정보취급자 및 정보주체의 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹 브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제, 카드번호 등 중요정보에 대한 복사·화면캡쳐 방지 및 키보드해킹 방지 등 보호대책을 적용하도록 계획하고 있습니까?			○	
평가근거 및 의견	● 대상시스템의 개인별 시험합격 조회 화면과 회원정보 수정 화면에서, 고유식별정보 입력 시 특정 자릿수가 임의의 문자로 대체 없이 중요 개인정보가 노출되고 있음.				

개인별 합격조회 화면	
회원정보 수정 화면	

관련법령 및 문서

관련 법령 · 지침

● 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

세부분야	출력 시 보호조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.8.3	● **개인정보취급자가 개인정보를 종이로 출력할 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책을 적용하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 출력물에 해당 기관의 명칭 및 로고, 일련 번호, 출력기기 고유번호, 출력자 성명, 출력시간을 표시하도록 설계하고 있으나 일부 내용이 누락된 경우				
평가근거 및 의견	● 개인정보취급자가 개인정보를 출력하면 사용자 이름, IP정보, 출력일자 및 시간 정도만 표시되고 나머지 기관명칭 및 로고, 일련번호, 출력기기 고유번호 등은 표시되지 않음				

주요 점검 사항

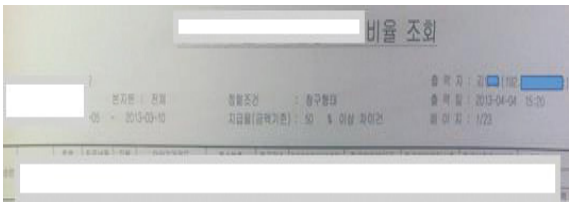
1. 개인정보를 종이로 출력하는 경우에는 출력물의 안전한 관리를 위한 보호조치를 적용하여야 한다.
   ① 출력기록 저장 및 보관
   ② 출력물에 출력자, 출력일시 표시 등

지표 해설

- 개인정보가 포함된 출력·복사물의 안전한 관리를 위해 관련 내용 기록 등의 보호조치를 취하여야 한다. 개인정보관리책임자는 출력·복사물의 보호조치를 위해 업무의 상황에 따라 기록할 정보를 정할 수 있지만, 출력·복사물의 책임관계 및 출처를 명확히 하기 위해 관련정보를 기록하여 관리할 것을 권장한다.
  - 출력/복사물의 책임관계 및 출처를 명확히 하기 위해 출력·복사 기록에는 출력자 부서/성명, 출력시간, 출력 파일명 등을 포함할 수 있고, 출력·복사물에 표시하는 출력자 정보는 해당 기관의 명칭 및 로고, 출력자 성명, 출력시간 등을 포함할 수 있다.
  - 응용프로그램을 통하여 출력하는 경우에는 출력기록은 '접속기록'에 포함하여 관리할 수 있다.
- 또한 개인정보가 포함된 종이 인쇄물을 통해 개인정보가 유출되지 않도록 개인정보의 출력·복사 기록 및 출력 및 복사 인쇄물에 출력자 정보를 기록하는 등의 보호조치를 적용하는 것을 권장한다.
  - 출력 및 복사 기록을 통해 출력/복사물의 생성, 이용, 전달, 파기 과정까지의 책임관계를 명확히 하여 사후 문서 유출 발생 시 출처를 확인할 수 있으며, 업무상 불필요한 개인정보 출력·복사를 억제하는 효과가 있다.
- 출력·복사 시 보호대책을 적용하기 위해 아래와 같은 보안기술을 활용할 수 있다.
  - 응응프로그램 기능 구현 : 응용프로그램을 통해 출력 시 워터마크 포함 출력
  - DRM 솔루션 : 일반적으로 DRM솔루션에서 출력물 워터마크 기능 제공함

- 출력보안 솔루션 : 출력 시 사용자 인증 및 이력관리, 출력물 워터마크 등
- 복합기보안 솔루션 : 사원증 등을 통한 사용자 인증, 출력·복사 등 통제

평가 예시

<table>
<tr><th>구 분</th><th>질의문</th><th>이행</th><th>부분이행</th><th>미이행</th><th>해당없음</th></tr>
<tr><td>4.8.3</td><td>개인정보취급자가 개인정보를 종이로 출력할 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책을 적용하도록 계획하고 있습니까?</td><td></td><td>○</td><td></td><td></td></tr>
<tr><td>평가근거 및 의견</td><td>● 개인정보취급자가 개인정보를 출력하면 사용자 이름, IP정보, 출력일자 및 시간 정도만 표시되고 나머지 기관명칭 및 로고, 일련번호, 출력기기 고유번호 등은 표시되지 않음
<table>
<tr><th>구분</th><th>기관의 명칭 및 로고</th><th>일련 번호</th><th>출력기기 고유번호</th><th>출력자 성명</th><th>출력시간</th><th>비고</th></tr>
<tr><td>수행여부</td><td>×</td><td>×</td><td>×</td><td>○</td><td>○</td><td>IP 정보</td></tr>
</table>
<table>
<tr><td>종이 출력 시 사용자 이름, IP정보, 출력일자 및 시간 등 일부 표시</td><td> 
</td></tr>
</table></td></tr>
</table>

관련법령 및 문서

관련 법령 · 지침

- 본 항목은 '개인정보 안전조치 의무'를 위한 기술적 보호 방법으로 개인정보의 안전한 보호를 위한 권장사항임

9 개인정보 처리구역 보호

세부분야	보호구역 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.9.1	● **개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 CCTV, 출입통제 장치, 화재경보기 등 보호설비를 설치·운영하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 보호구역을 지정하고 이에 관하여 문서로 확인할 수 있으나 일부 지역만 보호구역으로 지정한 경우, 혹은 보호구역 표시가 안되어 있는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 정보보안 기본지침 '제14조(중요 정보통신시설 등의 보안관리)'에 '전산기계실', '자료실'은 보호구역으로 지정하고 있으나 과거 자료를 보관하는 '문서고'는 보호구역으로 지정하고 있지 않음				

주요 점검 사항

1. 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하여야 한다.
2. 해당 보호구역에는 물리적·환경적 위협에 대응할 수 있도록 적절한 보호설비를 설치하고 운영하여야 한다.
   ① 출입통제 장치
   ② CCTV 등 감시장치
   ③ 서버랙 및 잠금장치
   ④ 화재경보기 등
   ※ 대상 기관에 별도의 물리 보안 규정이 있는 경우 해당 규정 준수 필요

지표 해설

- 개인정보를 대량으로 보관하고 있는 전산실·자료보관실 등 물리적 보관 장소를 별도로 두고 있는 경우, 비인가자의 물리적 접근 및 각종 물리적, 환경적 위협으로부터 개인정보처리시스템 등을 보호하기 위하여 해당 장소를 통제구역 등 보호구역으로 지정하고 적절한 보호대책을 수립·이행하여야 한다.
- 보호구역 지정 및 보호구역 내 물리적 접근통제는 내부 정책, 규정 등으로 문서화 되어 있거나, 보호구역 표시로 확인할 수 있다.

- 대상 기관의 물리적 보안과 관련된 규정이 있는 경우, 해당 규정에서 명시한 사항을 준수하여 통제 수준 및 방법을 결정할 필요가 있다(통제구역 표시방법, 출입 절차 등).
- 출입통제 절차 및 반·출입 통제절차는 영향평가 지표 4.6.1 및 4.6.2 참조

● 보호구역에 대한 보호대책은 아래 사항을 참고할 수 있다.

보호구역 보호대책 예시	
보호대책	설명
출입통제	- 출입통제 장치 : 비밀번호, 출입카드, 생체인식 등 - 출입통제 절차 마련 등
영상감시	- CCTV 및 영상저장장치(DVR, NVR 등) - 주요 작업 감시(출입, 개인정보처리시스템 접속, 개인정보 서류반출 등)
반·출입 통제	- 검색 장비 : 보안검색대(X-Ray검색대, 금속감지기 등) - 자산(장비, 보조저장매체, 노트북 등) 반·출입 절차
장비 배치 (서버RACK 등)	- 전산실 내에 다른 용도의 여러 장비가 함께 위치하는 경우(외부IDC 입주 등), 개인정보처리 시스템은 별도의 서버 RACK(잠금장치 포함)으로 구성하여 전산실 출입자라 하더라도 권한이 없는 인원은 접근하지 못하도록 통제
환경적 보호대책	- 화재 대책 : 화재경보기, 소화설비 - 온습도 대책 : 항온 항습기 - 누수 대책 : 누수감지기 - 전력 대책 : UPS 등
※ 위에서 제시된 모든 보호대책을 반드시 적용해야 하는 것은 아님, 다만 최소한 대상 기관의 물리적 보안 규정을 준수하여야 하며, 추가적으로 보호대책 미적용 시의 위험도 등을 고려하여 적절한 보호대책 선정할 필요가 있음 ※ 출입통제 및 반·출입 통제는 영향평가 지표 4.6.1, 4.6.2 참조	

● 개인정보 서류를 대량으로 보관하는 문서고의 경우에는 업무 및 개인정보 취급 권한에 따라 문서고 내 서류 보관을 별도로 구분하고, 허가된 취급자만 개인정보를 취급할 수 있도록 물리적인 통제를 적용할 것을 권장한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.9.1	개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 CCTV, 출입통제 장치, 화재경보기 등 보호설비를 설치·운영하도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관은 정보보안 기본지침 '제14조(중요 정보통신시설 등의 보안관리)'에 '전산기계실', '자료실'은 보호구역으로 지정하고 있으나 개인정보(회원가입 신청서)를 보관하는 '문서고'는 보호구역으로 지정하고 있지 않음.				

정보보안 기본지침	**제14조(중요 정보통신시설 등의 보안관리)** ①공단은 다음 각호의 중요 정보통신시설 및 장소를 보호구역으로 설정 관리하여야 한다. 1. 전산기계실 2. 자료실 ②이사장은 제1항에 따라 지정된 보호구역에 대해서는 보안대책을 강구하고 정기적으로 보안점검을 실시하여야 한다.

관련법령 및 문서

관련 법령 · 지침

- '보호구역 지정'은 법적 필수사항은 아니나 전산실, 자료보관실 등 개인정보를 보관하는 물리적 장소에 대하여 효과적인 출입통제 및 반·출입통제를 시행하기 위한 권장사항임

관련 문서

- 개인정보의 안전성 확보조치 기준 해설서 – 제11조 물리적 안전조치

세부분야	보호구역 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.9.2	● **개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 개인정보처리시스템에 대한 위기 대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검을 수행한 경우				
평가근거 및 의견	● ○○기관은 개인정보처리시스템 재해·재난 대비하여 긴급 재난복구 시행세칙을 수립하여 서버, 네트워크, 어플리케이션 등에 대한 재난 복구 절차를 마련하고 있으며, 2016년 재난복구 모의 훈련을 실시함				

주요 점검 사항

1. 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

지표 해설

- 재난이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것을 말하며, 재해란 재난으로 인하여 발생하는 피해를 말한다.
- 「재난 및 안전관리 기본법」 제3조(정의)에서 재난에 대한 용어 정의가 되어 있고, 「자연재해대책법」 제2조(정의)에 재해에 대한 용어 정의가 되어 있다.

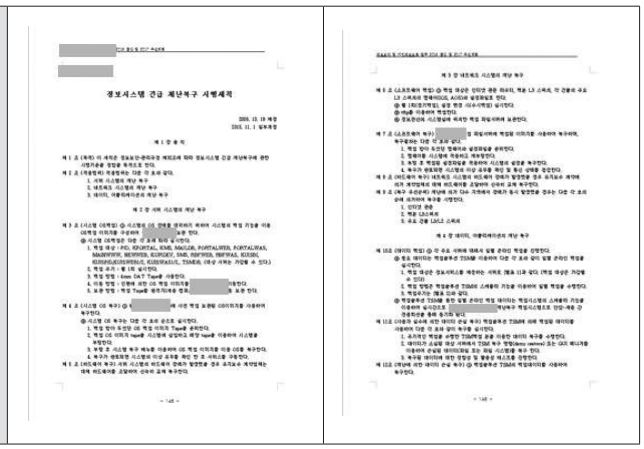
재난 및 안전관리 기본법 제3조(정의)
1. "재난"이란 국민의 생명 · 신체 · 재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각 목의 것을 말한다. 가. 자연재난: 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 낙뢰, 가뭄, 지진, 황사(黃砂), 조류 (藻類) 대발생, 조수(潮水), 화산활동, 소행성 · 유성체 등 자연우주물체의 추락 · 충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해 나. 사회재난: 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염 사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산 등으로 인한 피해

자연재해대책법 제2조(정의)
1. “재해”란 「재난 및 안전관리 기본법」 (이하 “기본법”이라 한다) 제3조제1호에 따른 재난으로 인하여 발생하는 피해를 말한다.

- 개인정보처리자는 재해 · 재난 발생 시 개인정보의 손실 및 훼손 등을 방지하고 개인정보 유출사고 등을 예방하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 문서화하여 마련하고 이에 따라 대처하여야 한다.

- 또한, 개인정보처리자는 대응절차의 적정성과 실효성을 보장하기 위하여 정기적으로 점검하여야 한다.
  - 대응절차를 정기적으로 점검하여 대응절차에 변경이 있는 경우에는 변경사항을 반영하는 등 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.9.2	개인정보처리자는 화재, 홍수, 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검하도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○기관은 개인정보처리시스템 재해·재난 대비하여 긴급 재난복구 시행세칙을 수립하여 서버, 네트워크, 어플리케이션 등에 대한 재난 복구 절차를 마련하고 있고, 2016년 재난복구 모의 훈련을 실시하고 있음 재해·재난 복구 절차 				

모의훈련	2-6. 제3차 재난복구 모의훈련 일자 / 업무처리 내역 2016.03.09 / 정보시스템 재난복구 모의훈련 시행(3차) 2016.04.05 / 정보시스템 재난복구 모의훈련 시행(3차) 결과 보고 ▣ 정보시스템 재난복구 모의 훈련(제3차) 1. 전체 이력 - 3차 : 2016년 3월 15일, [redacted]를 대상으로 진행 - 2차 : 2011년 8월 23일, [redacted]시스템)을 대상으로 진행 - 1차 : 2010년 8월 17일, [redacted]를 대상으로 진행 2. 3차 재난복구 모의 훈련 결과 요약 가. 훈련목적 ▪ 예기치 못한 재난상황에 대비 ▪ 재난발생 시 [redacted]의 정보서비스의 공백과 피해를 최소화 ▪ 최소시간 내 복구를 위한 훈련 ▪ 운영중인 재난복구 복구시스템을 운용한 실질적인 복구훈련 나. 훈련범위 ▪ [redacted] 데이터베이스(DB) 다. 훈련결과 ▪ 소요시간 ✓ OS 및 DB 데이터 복원(5시간) ✓ 포탈서비스 데이터베이스(DB) 구동(1시간) ✓ 복원 데이터 가용성 및 정합성 확인(1시간) ▪ 재난복구 모의훈련을 성공적으로 수행 ▪ [redacted]의 데이터베이스(DB) 백업데이터 가용성 및 정합성 확인 ▪ 직원들의 재난복구 프로세스 숙지 및 비상대응능력 강화

관련법령 및 문서

관련 법령 · 지침

【개인정보의 안전성 확보조치 기준 고시】

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

관련 문서

- 개인정보의 안전성 확보조치 기준 해설서 – 제12조 재해·재난 대비 안전조치치

세부분야	보호구역 지정				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.9.3	● **개인정보처리자는 재해 · 재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 재해·재난 발생 시 개인정보처리시스템에 대한 백업 및 복구를 위한 구체적인 계획이 마련되어 있는 경우				
평가근거 및 의견	● ○○기관은 개인정보처리시스템 재해·재난 대비하여 긴급 재난복구 시행세칙을 수립하고 있고, 재해·재난 대비하여 운영체제 및 DB에 대한 백업 및 복구절차를 마련하여 이행하고 있음				

주요 점검 사항

1. 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

지표 해설

● 개인정보처리자는 재해·재난 발생 시 혼란을 완화시키고 신속한 의사 결정을 위한 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

- 백업 및 복구를 위한 계획에는 개인정보처리시스템 등 백업 및 복구 대상, 방법 및 절차 등을 포함하도록 한다.

개인정보처리시스템 위기대응 매뉴얼 및 백업·복구 계획 예시
- 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등) - 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안 - 개인정보처리시스템 백업 및 복구 우선순위, 목표시점·시간 - 개인정보처리시스템 백업 및 복구 방안(복구센터 마련, 백업계약 체결, 비상가동 등) - 업무분장, 책임 및 역할 - 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
4.9.3	개인정보처리자는 재해 · 재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○기관은 개인정보처리시스템 재해·재난 대비하여 긴급 재난복구 시행세칙을 수립하고 있고, 재해·재난 대비하여 운영체제 및 DB에 대한 백업 및 복구절차를 마련하여 이행하고 있음				

백업 및 복구 계획	제 2 장 서버 시스템의 재난 복구 제 3 조 (시스템 OS백업) ① 시스템의 OS 장애를 대비하기 위하여 시스템의 백업 기능을 이용 OS백업 이미지를 구성하여 [redacted]에 보관 한다. ② 시스템 OS백업은 다음 각 호에 따라 실시한다. 1. 백업 대상 : [redacted] (대상 서버는 가감될 수 있다.) 2. 백업 주기 : 월 1회 실시한다. 3. 백업 방법 : 4mm DAT Tape을 사용한다. 4. 이동 방법 : 인편에 의한 OS 백업 이미지를 [redacted]까지 이동한다. 5. 보관 방법 : 백업 Tape를 원격지(세종 캠퍼스 내화금고)에 이동 보관 한다. 제 4 조 (시스템 OS 복구) ① [redacted]에 사전 백업 보관된 OS이미지를 사용하여 복구한다. ② 시스템 OS 복구는 다음 각 호의 순으로 실시한다. 1. 백업 받아 두었던 OS 백업 이미지 Tape을 준비한다. 2. 백업 OS 이미지 tape을 시스템에 삽입하고 해당 tape을 이용하여 시스템을 부팅한다. 3. 부팅 후 시스템 복구 메뉴를 이용하여 OS 백업 이미지를 이용 OS를 복구한다. 4. 복구가 완료되면 시스템의 이상 유무를 확인 한 후 서비스를 구동한다. 제 5 조 (하드웨어 복구) 서버 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약업체는 대체 하드웨어를 조달하여 신속히 교체 복구한다.

관련법령 및 문서

관련 법령 · 지침

【개인정보의 안전성 확보조치 기준 고시】

제12조(재해·재난 대비 안전조치)

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

관련 문서

- 개인정보의 안전성 확보조치 기준 해설서 – 제12조 재해·재난 대비 안전조치

5. 특정 IT기술 활용 시 개인정보보호

1 CCTV

세부분야	CCTV 설치 시 의견수렴				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.1.1	● **CCTV 설치시 관계 전문가 및 이해관계인의 의견을 수렴하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : CCTV 설치 시 관련 전문가 및 이해관계인의 의견수렴은 하고 있으나 일부 CCTV 설치 시에는 누락되어 있는 경우				
평가근거 및 의견	● A기관은 2013년에 설치한 CCTV에 대하여는 홈페이지 공지사항에 이해관계인의 의견수렴을 받았으나, 2012년 이전에 설치된 CCTV에 대해서는 관계 전문가 및 이해관계인의 의견수렴을 받지 않았음				

주요 점검 사항

1. 공공기관이 공개된 장소에 영상정보처리기기(이하 CCTV)를 설치하려는 경우에는 공청회 등을 통하여 관계 전문가 및 이해관계자의 의견을 수렴하여야 한다.
2. 아래의 경우를 제외하고는 CCTV를 공개된 장소에 설치하여서는 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
3. 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저하게 침해할 우려가 있는 장소의 내부를 볼 수 있도록 CCTV를 설치·운영하여서는 아니 된다.

지표 해설

- "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 의미한다.
- "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 다수(정보주체)가 접근 및 통행하는 데에 제한을 받지 아니하는 장소를 의미한다.

공개된 장소의 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, 주민 센터의 민원실 등 국가 또는 지방자치단체가 운영하는 시설로 민원인 또는 주민의 출입에 제한이 없는 공공기관 내부

- "비공개된 장소"인 경우에는 법 제15조제1항에 따라 정보주체의 동의나 법률에 특별한 규정이 있는 경우 등에만 영상정보처리기기의 설치·운영(개인영상정보의 수집 및 이용)이 가능하다.

비공개 장소의 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

- 공개된 장소에서의 영상정보처리기기 설치는 원칙적으로 금지되고, 예외적으로 「개인정보 보호법」 제25조에서 정하는 사유에 해당하는 경우에만 영상정보처리기기를 설치·운영할 수 있다.(법 제25조제1항)

공개된 장소에 영상정보처리기기 설치가 가능한 경우
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

- 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 금지된다.(법 제25조제2항)
- 다만, 교도소, 정신보건시설 등과 같이 법령에 근거하여 사람을 보호하는 시설로서 대통령령으로 정한 시설에 대해서는 예외적으로 영상정보처리기기를 설치·운영 할 수 있다.(법 제25조제2항)

개인의 사생활을 현저히 침해할 우려가 있는 장소의 예외적 설치·운영 허용 예
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

- 영상정보처리기기의 무분별한 설치·운영 및 이로 인한 사생활 침해를 방지하기 위하여 설치·운영 시 관계인의 의견을 수렴하여 반영할 필요가 있다.
- 공공기관이 공개된 장소에 영상정보처리기기를 설치운영하려는 경우에는 다음의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.
  - 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
  - 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사
- 영상정보처리기기의 설치 목적 변경 및 추가 설치 등의 경우에도 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다. 다만 동일 목적 내 단순히 추가적으로 설치하는 경우에는 의견 수렴을 하지 않을 수 있다.(표준지침 제42조)
- 「개인정보 보호법」 제25조제2항 및 영 제22조에 따른 교정시설이나 정신의료기관 등에 영상정보처리기기를 설치·운영하려는 자는 다음의 사람으로부터 모두 의견을 수렴하여야 한다.
  - 관계 전문가
  - 해당시설에 종사하는 사람, 해당시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.1.1	CCTV 설치 시 관계 전문가 및 이해관계인의 의견을 수렴하도록 계획하고 있습니까?		○		
평가근거 및 의견	● A기관은 2013년에 설치한 CCTV에 대하여는 홈페이지 공지사항에 이해관계인의 의견수렴을 받았으나, 2012년 이전에 설치된 CCTV에 대해서는 관계 전문가 및 이해관계인의 의견수렴을 받지 않았음				

CCTV 이해관계인 의견 수렴 공지	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

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, 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 대해서는 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.

【개인정보 보호법 시행령】

제23조(영상정보처리기기 설치 시 의견 수렴) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 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 설명회·설문조사 또는 여론조사

② 법 제25조제2항 단서에 따른 시설에 영상정보처리기기를 설치·운영하려는 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

【표준 개인정보 보호지침】

제38조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제25조
- 공공기관 영상정보처리기기 설치 · 운영 가이드라인
- 민간분야 영상정보처리기기 설치 · 운영 가이드라인

세부분야	CCTV 설치 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.1.2	● **CCTV 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판 설치하거나 홈페이지, 이메일 등을 통해 안내하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : CCTV 설치에 대한 안내판 설치 등의 안내를 하고 있으나 안내내용이 적절하지 못한 경우				
평가근거 및 의견	● CCTV에 대한 운영을 위탁하고 CCTV 설치에 대한 안내판은 설치되어 있으나, 안내판 내용 중 위탁받은 자의 명칭 및 연락처가 누락되어 있음				

주요 점검 사항

1. 공개된 장소에 CCTV를 설치·운영하는 경우에는 정보주체가 쉽게 확인할 수 있도록 안내판 설치 등 필요한 조치를 하여야 한다.
   ① 설치 목적 및 장소
   ② 촬영 범위 및 시간
   ③ 관리책임자의 성명 및 연락처
   ④ (위탁 시)위탁받는 자의 명칭 및 연락처
2. 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 위치에 설치되어야 한다.
3. 교통 단속 등 개인정보 침해의 우려가 적거나, 산불 단속 등 장소적 특성으로 인하여 안내판 설치가 불가능한 경우에는 홈페이지를 통해 관련 내용을 게재하는 것으로 안내판 설치를 갈음할 수 있다.

지표 해설

- 영상정보처리기기는 공개된 장소에 지속적으로 설치·운영되고 있으므로, 촬영 대상자는 자기의 모습이 촬영되는지에 대해 통제권을 행사하는 것이 사실상 불가능하다. 따라서 법 제25조의 적용을 받는 영상정보처리기기에 대해서는 그 촬영사실을 알리는 안내판 설치를 통해 촬영대상자의 개인정보자기결정권을 보장하는 것이 필요하다.
- 영상정보처리기기운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 안내판을 설치하여야 한다. 안내판 기재 항목은 다음과 같다.

영상정보처리기기 안내판 기재사항
1. 설치목적 및 장소 2. 촬영범위 및 시간 3. 관리책임자 및 연락처 4. (영상정보처리기기 설치·운영을 위탁한 경우) 위탁받는 자의 명칭 및 연락처

- 백화점, 역사 등 규모가 큰 건물의 경우에는 다수의 영상정보처리기기가 설치되어 있는데, 이러한 각각의 기기에 대해 개별적으로 안내판 설치를 강제하는 것은 과도한 규제가 될 수 있다. 따라서 건물 안에 다수의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.(영 제24조제1항 단서)

- 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독될 수 있게 설치되어야 하고, 이를 충족하였다면 그 범위 내에서 안내판의 크기나 설치위치는 영상정보처리기기 운영자가 자율적으로 정할 수 있다.(표준지침 제39조제2항)

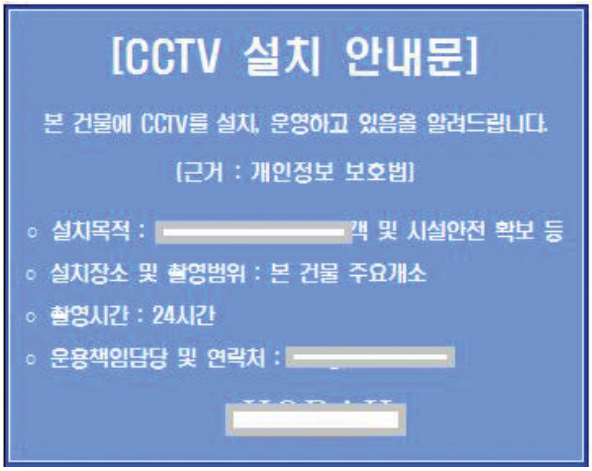
- 공공기관은 영상정보처리기기의 효율적 관리와 정보 연계를 위해 통합 관리하는 경우가 있다. 이러한 때에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제45조제1항에 따른 안내판에 기재하여야 한다.(표준지침 제39조제3항)

● 영상정보처리기기의 운영현황에 따라서는 안내판을 설치하는 것이 의미가 없거나 정보주체가 알아볼 수 없는 상황이 있을 수 있다. 따라서 법에서는 ① 공공기관이 원거리촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보침해의 우려가 적은 경우 또는 ② 영상정보처리기기 운영자가 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 이를 쉽게 알아볼 수 없는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 영 제24조제1항 각 호의 사항을 게재할 수 있도록 하였다.

● 소규모 사업자나 소상공인 등은 아예 인터넷 홈페이지가 없는 경우가 있을 수 있다. 이처럼 영상정보처리기기 운영자가 인터넷 홈페이지에 게재사항을 게재할 수 없는 경우에는 ① 영상정보처리기기 운영자의 사업장·영업소·사무소·점포 등(이하 "사업장등"이라한다)의 보기 쉬운 장소에 게시하거나 ② 관보(영상정보처리기기 운영자가 공공기관인 경우로 정한다)나 영상정보처리기기 운영자의 사업장등이 소재하는 특별시·광역시·도 또는 특별자치도(이하 "시·도"라 한다) 이상의 지역의 주된 보급지역으로 하는 「신문등의 진흥에 관한 법률」 제2조제1호·제2호에 따른 일반 일간신문, 일반 주간신문 또는 인터넷 신문에 싣는 방법으로 게재사항을 공개하여야 한다.(영제24조제2항)

- 국가안보 등 중대한 공익적 목적을 위해 설치·운영되는 영상정보처리기기에 대해서는 안내판 설치가 오히려 그 목적 달성에 장애가 될 수도 있다. 따라서 이러한 시설에 대해서는 안내판 설치의 면제가 필요하다. 즉 공공기관의 장이 ①「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, ②「통합방위법」 제2조제13호에 따른 국가중요시설, ③「보안업무규정」 제36조에 따른 보안 목표시설에 영상정보처리기기를 설치할 때에는 안내판을 설치하지 아니할 수 있다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.1.2	CCTV 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나 홈페이지, 이메일 등을 통해 안내하도록 계획하고 있습니까?		○		
평가근거 및 의견	● CCTV에 대한 운영을 위탁하고 CCTV 설치에 대한 안내판은 설치되어 있으나, 안내판 내용 중 위탁받는 자의 명칭 및 연락처가 누락되어 있음 CCTV 설치 시 안내판  				

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제25조(영상정보처리기기의 설치·운영 제한)

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 「군사기기 및 군사시설 보호법」 제2조제2호에 다른 군사시설, 「통합방위법」 제2조제13호에 따른 국가 중요시설, 그 밖에 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

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

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.

【개인정보 보호법 시행령】

제24조(안내판의 설치 등) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 영상정보처리기기가 설치·운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 같은 조 제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

② 제1항에도 불구하고 영상정보처리기기운영자가 설치·운영하는 영상정보처리기기가 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 있다.

1. 공공기관 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 법 제25조제4항 각 호의 사항을 게재할 수 없으면 영상정보처리기기운영자는 다음 각 호의 어느 하나 이상의 방법으로 법 제25조제4항 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 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목 · 다목 또는 같은 조 제2호에 따른 일반일간신문 · 일반주간신문 또는 인터넷신문에 싣는 방법

④ 법 제25조제4항 각 호 외의 부분 단서에서 "대통령령으로 정하는 시설"이란 「보안업무규정」 제32조에 따른 국가보안시설을 말한다.

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 확보조치에 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.

【표준 개인정보 보호지침】

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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제25조
- 공공기관 영상정보처리기기 설치 · 운영 가이드라인
- 민간분야 영상정보처리기기 설치 · 운영 가이드라인

세부분야	CCTV 사용 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.1.3	● **CCTV 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : CCTV 임의조작 및 음성녹음기능을 금지하도록 적용하고 있는 경우				
평가근거 및 의견	● A기관은 개인정보보호지침 내 임의조작 및 음성녹음 할 수 없음을 명시하고 있고, 전산실 출입구 앞, 1층 로비, 각 사무실 입구 앞 등에 CCTV(모델 DF4510HD)가 설치되어 있으며, 해당 제품은 녹음기능이 없고, 고정형으로 설치되어 임의조작이 되지 않도록 운영하고 있음				

주요 점검 사항

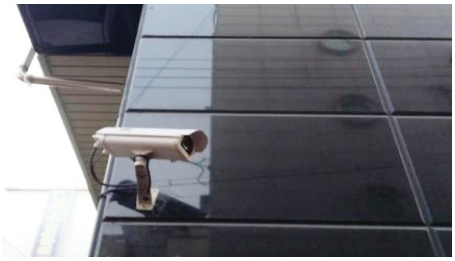
1. CCTV를 설치 목적과 다른 목적으로 임의로 조작하거나 다른 곳을 비추어서는 안 된다.
2. CCTV는 녹음기능을 사용하여서는 안 된다.

지표 해설

- 영상정보처리기기는 일정한 장소에 지속적으로 설치·운영되고 있으므로, 만일 음성, 음향을 녹음하는 기능을 갖추고 있다면 본의 아니게 사람들간의 대화를 녹음하는 결과를 가져온다. 그러나 타인간의 대화를 청취·녹음하는 행위는「통신비밀보호법」에서 엄격히 금지하고 있으므로(제3조), 이 법에 따른 영상정보처리기기는 녹음기능을 제한할 필요가 있다.
- 또한 운영자에 의한 임의조작을 가능하게 할 경우에도 역시 사생활 침해의 우려가 커진다. 따라서 이 법은 영상정보처리기기 운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비출 수 없도록 하고, 녹음기능 역시 사용할 수 없도록 규정하고 있다.(법 제25조제5항)

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.1.3	CCTV 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 계획하고 있습니까?	○			
평가근거 및 의견	● A기관은 개인정보보호지침 제46조(개인영상정보 이용제3자 제공 및 제한 등) 내 임의조작 및 음성녹음 할 수 없음을 명시하고 있고, 전산실 출입구 앞, 1층 로비, 각 사무실 출입구 앞 등에 CCTV(모델 DF4510HD)가 설치되어 있으며, 해당 제품은 녹음기능이 없고, 고정형으로 설치되어 임의조작이 되지 않도록 하고 있음				

개인정보보호 지침 제46조	제46조(개인영상정보 이용 · 제3자 제공 및 제한 등) ① 개인영상정보 운영담당은 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 외로 이용하거나 제3자에게 제공하여서는 아니 된다. ⑤ 개인영상정보 운영담당은 설치목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.
CCTV 설치	

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제25조(영상정보처리기기의 설치·운영 제한) ⑤ 영상정보처리기기운영자는 영상정보처리 기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제25조
- 공공기관 영상정보처리기기 설치 · 운영 가이드라인
- 민간분야 영상정보처리기기 설치 · 운영 가이드라인

세부분야	CCTV 사용 제한				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.1.4	● **CCTV 운영 시 CCTV에 대한 운영·관리방침을 수립하도록 하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : CCTV 운영·관리방침 수립을 계획하고 있으나 내용일부가 누락되어 있는 경우				
평가근거 및 의견	● A기관 CCTV 운영·관리방침 내 '정보주체의 영상정보 열람 등 요구에 대한 조치', '영상정보의 보호를 위한 기술적·관리적·물리적 조치'에 대한 부분이 누락되어 있음				

주요 점검 사항

1. CCTV 운영 시, '영상정보처리기기 운영·관리 방침'을 마련하여 인터넷 홈페이지 등에 공개하여야 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

지표 해설

● 영상정보처리기기 운영자는 다음 각 호의 사항이 포함된 영상정보처리기 운영·관리 방침을 마련하여야 한다.

영상정보처리기기 운영·관리 방침에 포함되어야 할 사항
1. 영상정보처리기기의 설치 근거 및 설치 목적 2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위 3. 관리책임자, 담당 부서 및 영상정보에 관한 접근 권한이 있는 사람 4. 영상정보의 촬영 시간, 보관 기간, 보관 장소 및 처리 방법 5. 영상정보처리기운영자의 영상정보 확인 방법 및 장소 6. 정보주체의 영상정보 열람 등 요구에 대한 조치 7. 영상정보의 보호를 위한 기술적·관리적·물리적 조치 8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

- 영상정보처리기기운영자가 영상정보처리기기 운영관리 방침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다(법 제25조제7항). 또한 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.(표준지침 제40조제2항)
- 영상정보처리기기운영자가 영상정보처리기 운영·관리 방침을 정한 경우에는 이를 공개하여야 한다. 공개에 관하여는 시행령 제31조제2항 및 제3항(개인정보 처리방침의 공개방법)을 준용한다(영 제25조제2항). 즉, 영상정보처리기기 운영·관리 방침은 원칙적으로 영상정보처리기기 운영자의 인터넷 홈페이지에 지속적으로 게재해야 하며, 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 영상정보처리기기 운영·관리 방침을 공개해야 한다.

영상정보처리기기 운영·관리 방침 공개 방법
1. 개인정보처리자의 사업장 등의 보기 쉬운 장소에 게시하는 방법 2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장 등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷 신문에 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

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.1.4	CCTV 운영 시 CCTV에 대한 운영·관리방침을 수립하도록 계획하고 있습니까?		○		
평가근거 및 의견	● A기관은 개인정보 보호법 시행령 제25조제1항에 따른 CCTV 운영·관리 방침 내용 중 '정보주체의 영상정보 열람 등 요구에 대한 조치', '영상정보의 보호를 위한 기술적·관리적·물리적 조치'에 대한 부분이 누락되어 있음				

CCTV 운영·관리 방침	【 영상정보처리기기 운영·관리 방침 】 OOO재단(이하 재단이라 함)는 영상정보처리기기 운영·관리 방침을 통해 본 기관에서 처리하는 영상정보가 어떠한 용도와 방식으로 이를 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 - 차량도난 및 파손방지 **2. 설치 대수, 설치 위치 및 촬영범위** 설치 대수 / 설치 위치 및 촬영 범위 oo대 / 본사(건물외벽, 주차장 입구) oo대 / 사옥소(건물외벽, 로비) **3. 관리책임자 및 접근권한자** 귀하의 영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자를 두고 있습니다. 이름 / 직위 / 소속 / 연락처 관리책임자 접근권한자 **4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법** 촬영시간 / 보관기간 / 보관장소 24시간 / 촬영일로부터 oo일 / - 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. 개인영상정보의 확인 방법 및 장소에 관한 사항** - 확인 방법 : 영상정보 관리책임자에게 미리 연락하고 본 기관을 방문하시면 확인 가능합니다. - 확인 장소 : OOO부 **6. 영상정보처리기기 운영·관리방침 변경에 관한 사항** 이 영상정보처리기기 운영·관리방침은 2014년 4월 04일에 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. - 시행일자 : 2014년 4월 4일

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제25조(영상정보처리기기의 설치·운영 제한)

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

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.

【개인정보 보호법 시행령】

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, "개인정보 처리방침"은 "영상정보처리기기 운영·관리 방침"으로 본다.

【표준 개인정보 보호지침】

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 개인영상정보의 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제25조
- 공공기관 영상정보처리기기 설치 · 운영 가이드라인
- 민간분야 영상정보처리기기 설치 · 운영 가이드라인

세부분야	CCTV 설치 및 관리에 대한 위탁				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.1.5	● **CCTV 관리 위탁 시 개인정보보호에 필요한 전문 장비 및 기술을 갖춘 기관을 선정하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : CCTV 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관으로 선정하도록 계획하고 있으나 기관과의 계약문서에 내용이 적절하지 않은 경우				
평가근거 및 의견	● A기관은 개인정보보호지침 제49조와 CCTV 관리 위탁 입찰 시 업체자격 조건을 명시하여 선정하였으나, 계약문서의 경우 표준계약서에 따라 계약하여 개인정보 보호법 시행령 제26조에 위탁 계약 시 포함되어야 할 내용이 미흡함				

주요 점검 사항

1. CCTV 관리 업무를 위탁하는 경우 개인정보보호에 전문성이 있는 업체를 선정하도록 하여야 한다.
2. CCTV 관리 업무를 위탁하는 경우 위탁 계약서 등에 개인정보보호 관련 내용이 포함되도록 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

지표 해설

● 영상정보처리기기 설치·운영은 직접 하는 경우도 있지만, 상당수는 외부의 전문업체에 설치·운영을 위탁하는 형태로 이루어지고 있다. 이러한 운영 현실을 감안하여, 이 법은 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있도록 허용하고 있다.(법 제25조제8항)

공공기관 영상정보처리기기 설치·운영 위탁 시 문서 포함사항
1. 위탁하는 사무의 목적 및 범위 2. 재위탁 제한에 관한 사항 3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 4. 영상정보의 관리현황 점검에 관한 사항 5. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

- 다만, 민간업체·단체·개인이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 위탁방법 등에 관하여 특별한 제한을 두고 있지 않으므로, 결과적으로 이 법 제26조(업무위탁에 따른 개인정보의 처리 제한)의 규정이 적용된다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.1.5	CCTV 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 계획하고 있습니까?		○		
평가근거 및 의견	● A기관은 개인정보보호지침 제49조와 CCTV 관리 위탁 입찰 시 업체자격 조건을 명시하여 자격조건에 부합한 업체를 선정하였으나, 계약문서의 경우 표준계약서에 따라 계약하여 손해배상 부분을 제외하고 개인정보 보호법 시행령 제26조에 따른 위탁 계약에 포함되어야 할 내용이 포함되어 있지 않음				

개인정보 보호지침 제49조	**제49조(영상정보처리기기 설치 및 관리 등의 위탁)** ① 개인영상정보 운영담당은 영상정보처리기기의 설치 · 운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 안내판 및 영상정보처리기기 운영 · 관리 방침에 수탁자의 명칭 등을 공개하여야 한다. ② 개인영상정보 운영담당은 영상정보처리기기의 설치 · 운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리 · 감독하여야 하며, 수탁자 관련 및 관련 사무는 제25조부터 제27조까지 준용한다.
입찰 시 업체자격 조건 명시	가. 건 명 : [redacted] 통합감시업무 용역(용역 및 1차) 나. 현 지 : 서울시 [redacted] 통합감시실 다. 목 적 : [redacted] 설치된 CCTV를 통하여 시설물 감시 및 이례상황 시 신속한 정보 제공으로써 고속전철자손해의 안전성을 도모하고 국민의 생명과 재산을 보호하고자 함 라. 계약 개요 : 통합감시실에서 실시간 CCTV를 감시하여 이례상황(Event) 발생 시 신속한 초동대응(현장대응 및 관련의 통보 및 조치, 장비장비 및 설비의 관리 마. 계약 방법 - 제공형태 : 용역계약 바. 계약 기간 [redacted] 2013. 01. 02. ~ 2015. 12. 30 사. 기타 사항 - 업무인원 : 7명(관장1, 감시요원6) - 업무이행시간 : 통합감시실근무자(이하 "감시자" 라 한다)는 매 24시간 업무의 단절 없이 교대로 근무함을 원칙으로 하되 근무시간은 ('갑) 와 ('을) 상호간에 협의에 의하여 조정할 수 있다. - 법률과계 : 정보통신법(법률 제9579호, '09. 4. 1) 제4조에 의거 '기술용역업' 의 허가를 받은 자
표준계약서	**표준 계약서** 주식회사 OOO(이하'갑'이라 한다)와 OOO(이하'을'이라 한다) 용역사업을 의뢰하고 '을'이 수행하는데 있어 다음과 같이 합의한다. **제 1 조 목적** 본 계약은 '고객사'의 CCTV 운영 및 관리를 위하여 '을'이 제공하는 사업과 관련된 제반 계약사항을 규정함을 목적으로 한다. **제 2 조 계약기간 및 조건** ① 본 계약은 2013년 01월 02일로부터 2013년 12월 31일까지로 한다. ② 본 계약은 '갑'과 '을' 상호간 사전 서면동의 없이 본 계약의 의무나 권리를 양도하거나 변경 또는 재계약하지 못한다. ③ 본 계약은 계약 기간 중이라도 변경 사유가 있을 경우 '갑'과 '을' 상호 합의에 따라 수정할 수 있으며, 양 당사자는 수정 조항에 대하여 본 계약서와 같은 인감으로 상호 날인하여 본 계약서에 첨부한다.

관련법령 및 문서

관련 법령 · 지침

【개인정보 보호법】

제25조(영상정보처리기기의 설치·운영 제한)

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.

【개인정보 보호법 시행령】

제26조(공공기관의 영상정보처리기기 설치·운영사무의 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.

【표준 개인정보 보호지침】

제43조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 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.

관련 문서

- 개인정보 보호법령 및 지침 · 고시 해설서 – 제3장 제25조
- 공공기관 영상정보처리기기 설치 · 운영 가이드라인
- 민간분야 영상정보처리기기 설치 · 운영 가이드라인

2 RFID

세부분야	RFID 이용자 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.1	● **RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : RFID 태그에 기록된 개인정보 수집 시 이용자에게 통지하지 않거나 알아보기 쉽게 표시하지 않은 경우				
평가근거 및 의견	● ○○의료원에서는 환자관리를 위해 비상시 필요한 의료정보, 과거 환자의 치료기록, 약물치료 등 의료기록 및 인적사항이 기록된 RFID 진료카드를 발급하였으나, 수집 시 환자에게 통지하거나 알아보기 쉽게 표시하고 있지 않음				

주요 점검 사항

1. RFID 태그에 기록된 개인정보를 수집하는 경우에는 해당 정보주체에게 통지하거나 알아보기 쉽게 표시하고 명시적 동의를 받아야 한다.

지표 해설

- 개인정보보호의 일반 원칙에 따르면 RFID 태그에 기록된 개인정보를 수집하고자 하는 경우에도 RFID 취급사업자는 수집목적 및 이용목적을 고지하고 동의를 획득하여야 한다.
- RFID 취급사업자는 이용자 보호를 위하여 RFID 태그에 개인정보 기록 시 당해 개인정보의 수집 및 이용이 예정되어 있는 경우 사전에 기록된 개인정보의 수집 목적 및 이용 목적, 수집방법 등에 대해 고지하고 동의를 획득하도록 하고, 실제 개인정보를 수집하는 경우에는 수집 사실 및 방법 등을 이용자에게 통지하거나 표시하여야 한다.

통지 또는 표시 내용
- RFID 태그에 기록된 개인정보의 수집 사실 및 방법 - 개인정보 보호책임자의 성명·연락처 등 - 이용자의 권리 또는 개인정보의 수집 및 이용에 관한 문의 등을 통해 통지 또는 표시의 목적을 현실적으로 달성할 수 있도록 조치

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.1	RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하도록 계획하고 있습니까?			○	
평가근거 및 의견	● A업체에서는 환자관리를 위해 비상시 필요한 의료정보, 과거 환자의 치료기록, 약물치료 등 의료기록 및 인적사항이 기록된 RFID 진료카드를 발급하였으나, 진료카드 발급 시 기록되는 ○○병원 진료차트의 개인정보 수집사항에 대하여 환자에게 통지하거나 안내하지 않음.				

RFID 진료카드	

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제4조(개인정보 기록의 금지 등) ① RFID 취급사업자는 RFID 태그에 개인정보를 기록하여서는 아니 된다. 다만 법률에 정한 경우 또는 서면 등을 통한 이용자의 명시적인 동의가 있는 경우는 그러하지 아니하다.

② RFID 취급사업자는 제1항 규정에 의한 동의를 얻고자 하는 경우에는 당해 이용자에게 미리개인정보의 기록목적 및 이용목적 등을 고지하여야 한다.

제5조(RFID 태그를 통한 개인정보의 수집) RFID 취급사업자는 제4조제1항 규정의 RFID 태그에 기록된 개인정보를 수집하는 경우에는 당해 이용자에게 이를 통지하거나 또는 쉽게 알아볼 수 있는 방법으로 표시하여야한다.

관련 문서

● RFID 프라이버시 보호 가이드라인 해설서 – 제2장 제5조

세부분야	RFID 이용자 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.2	● **RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : RFID 태그에 물품정보 등과 개인정보를 연계 시 이용자에게 통보하지 않거나 알아보기 쉽게 표시하지 않은 경우				
평가근거 및 의견	● ○○기관은 우편물 발송 시 우편물정보(발신자/수신자, 주소, 연락처 등)을 우편물의 무게, 용량 등의 물품정보와 함께 RFID 태그(전자추적표)에 담아 우편물에 부착하여 배송상태를 추적·관리하고 있으나, 관련 내용을 이용자에게 통지하지 않았음				

주요 점검 사항

1. RFID 태그의 물품정보 등과 개인정보를 연계하는 경우에는 그 사실을 해당 정보주체에게 통지하거나 알기 쉽게 표시하여야 한다.

지표 해설

- 이용자의 프라이버시 보호를 위하여 RFID 취급사업자는 RFID에 기록되어 있는 물품정보와 개인정보가 연계될 경우, 미리 그 사실을 이용자에게 통지하거나 알기 쉬운 방법으로 표시하여야 한다.
  - 통지 예시 : 회원가입신청서나 도서대출신청서 등을 작성할 때 서면으로 다른 고지 사항과 함께 통지
  - 표시 예시 : 이용약관 등에 해당 내용을 굵은 글씨나 색으로 강조하여 알아보기 쉽게 표시

통지 또는 표시 내용
- RFID 태그정보와 ○ ○○ 개인정보가 연계된다는 사실 - 개인정보 보호책임자의 성명·연락처 등 ※ 이용자의 권리 또는 개인정보의 수집 및 이용에 관한 문의 등을 통해 통지 또는 표시의 목적을 현실적으로 달성할 수 있도록 조치 필요

- RFID의 물품정보 등과 개인정보가 연계되어 생성된 정보(구매 패턴, 관심 품목, 소비지출 규모 등)를 이용하고자 하는 경우에는 개인정보 보호 원칙에 따라 이용목적을 고지하고 동의를 획득하여야 하므로 RFID 태그의 물품정보 등과 개인정보가 연계되어 특정 정보를 생성하는 것이 예정되어 있는 경우 또는 개인정보 수집 시에는 RFID 태그의 물품정보 등과 개인정보의 연계가 예정되지 않았으나 사후에 수집한 개인정보와 연계, 활용하고자 하는 경우 RFID 취급사업자는 다음과 같은 안내를 하고 동의를 받아야 한다.

- 최초 당해 개인정보 수집 시에 개인정보와 RFID 태그의 물품정보 등이 연계되어 특정 정보를 생성한다는 사실, 생성되는 정보 항목(구매 패턴, 관심 품목, 소비 지출 규모 등) 및 생성 목적(타겟 마케팅 등) 등을 미리 고지하고 동의를 획득하여야 한다.

고지 내용
- RFID 태그정보의 물품정보 등과 개인정보가 연계되어 특정 정보가 생성된다는 사실 - 생성되는 정보 항목 및 생성 목적 - 개인정보 보호책임자의 성명·연락처 등 ※ 이용자의 권리 또는 개인정보의 수집 및 이용에 관한 문의 등을 통해 통지 또는 표시의 목적을 현실적으로 달성할 수 있도록 조치 필요

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.2	RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기하도록 계획하고 있습니까?	○			
평가근거 및 의견	● ○○○은 구매판매 목록과 고객정보를 연계하여 고객의 물품에 대한 선호도를 파악, 마케팅 및 홍보의 목적으로 이용을 하고 있으며, 관련 사실의 내용을 고객에게 안내하고 동의를 받고 있음.				

RFID 개인정보 수집 · 이용 동의서	
	■ 회원님이 구매하시는 제품에는 RFID 태그가 부착 또는 내장되어 있으며, 이는 회원정보와 연계되어 회원님의 물품에 대한 선호도를 파악, 회원님이 선호하는 신제품 출시나 세일정보 등을 알려드리는데 사용됩니다. ■ 기타 사항은 개인정보관리책임자 △ △ △ (OO-OO-OOOO)에게 문의하여 주시기 바랍니다. 본인은 (갑)이 제공하는 회원서비스를 이용하기 위해 위의 사실에 따라 개인정보를 수집.이용하는데 동의합니다. 2007년 월 일 제공자 : (서명) 귀중

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제6조(RFID 태그의 물품정보 등과 개인정보의 연계) ① RFID 취급사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우에는 미리 그 사실을 당해 이용자에게 통지하거나 쉽게 알아볼 수 있는 방법으로 표시하여야 한다.

관련 문서

- RFID 프라이버시 보호 가이드라인 해설서 - 제2장 제6조

세부분야	RFID 이용자 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.3	● **RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : RFID 태그에 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집목적 외의 용도로 이용하거나, 제3자 제공 시 이용자의 동의를 얻도록 계획하지 않은 경우				
평가근거 및 의견	● ○○기관은 미아방지 목적으로 놀이공원 내에 설치된 리더기를 통해 RFID 태그 내 기록된 이름, 태그고유번호 등을 수집하고, 미아 발생 시 관한 경찰서로 이름, 주소 등 개인정보를 제공하고 있으나, 개인정보 수집·이용에 대한 동의 외 제3자 제공에 대한 동의를 받지 않음				

주요 점검 사항

1. RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공하려는 경우에는 해당 정보주체의 동의를 받아야 한다.

지표 해설

● 당초 동의한 목적 외 이용이나 제3자 제공을 할 경우에는 반드시 해당사실에 대해 추가 고지하고 동의를 획득하여야 한다. 〈RFID 프라이버시 보호 가이드라인 해설서〉

고지 내용
- RFID 태그의 물품정보 등과 개인정보가 연계되어 특정 정보가 생성된다는 사실 - 생성되는 정보 항목 및 생성 목적 - 개인정보관리책임자의 성명·연락처 등 ※ 이용자의 권리 또는 개인정보의 수집 및 이용에 관한 문의 등을 통해 고지의 목적을 현실적으로 달성할 수 있도록 조치 필요

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.3	RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○기관은 미아방지 목적으로 놀이공원 내에 설치된 리더기를 통해 RFID 태그 내 기록된 이름, 태그고유번호 등을 수집하고, 미아 발생 시 관할 경찰서로 이름, 주소 등 개인정보를 제공하고 있으나, 개인정보 수집·이용에 대한 동의 외 제3자 제공에 대한 동의를 받지 않음.				

RFID 개인정보 수집 · 이용 동의서	[동의 전 고지사항] ■ 개인정보의 기록 목적 : 미아방지 ■ 기록되는 개인정보 항목 : 이름, 태그 고유번호 ■ 개인정보 수집 · 이용 목적 및 수집방법 : 미아의 위치확인을 위해 놀이공원 내 설치된 리더기를 통해 RFID 태그 내 기록된 정보 수집 ■ 개인정보관리책임자 △ △ △ (○○-○○-○○○○) 본인은 (갑)이 제공하는 서비스를 이용하기 위해 위의 사실을 확인하고 개인정보를 기록하는데 동의합니다. 년 월 일 제공자 : (서명) 귀중

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제6조(RFID 태그의 물품정보 등과 개인정보의 연계) ② RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 당초의 수집목적 외로 이용하거나 제3자에게 제공하는 경우에는 이용자의 동의를 얻어야 한다.

제15조(개인정보 이용·제공·파기 등) 이 가이드라인에 정한 사항 외의 개인정보의 이용·제공·파기 및 이용자의 권리 보호 등 개인정보 보호와 관련한 사항은 정보통신망 이용촉진 및 정보보호 등에 관한 법령 및 지침의 개인정보보호 원칙에 따른다.

관련 문서

● RFID 프라이버시 보호 가이드라인 해설서 – 제2장 제6조, 제4장 제15조

세부분야	RFID 이용자 안내				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.4	● **RFID태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 안내사항이 적절하지 않거나 이용자가 쉽게 이해하기 힘들게 표기된 경우				
평가근거 및 의견	● ○○기관은 보안을 위해 기관 방문자에게 방문자의 이름, 연락처, 소속기관 등 개인정보가 담긴 RFID 카드를 발급하였고, 중요 시설공간에 리더기가 설치되어 있으나, 리더기 설치 사실을 안내하고 있지 않음				

주요 점검 사항

1. RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우에는 설치사실을 정보주체가 쉽게 인식할 수 있도록 표기하여야 한다.

지표 해설

- RFID 태그가 부착 또는 내장되어 이용자에게 교부된 물품에 대한 정보 또는 RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우에는 리더기가 설치되어 있다는 사실을 이용자가 용이하게 인식할 수 있게 표시하도록 하여 이용자가 자신의 중요한 개인정보가 누출되는 것을 사전에 방지할 수 있는 기회를 부여하여야 한다.
- 리더기 설치의 표시는 원칙적으로 리더기가 설치된 장소에 표시하는 것이 가장 바람직하며, 그 장소에 표시하는 것이 곤란한 경우에만 안내문 등을 통해 리더기의 설치장소를 이용자가 쉽게 알 수 있도록 하여야 한다.
  - 리더기 설치 장소에 인식하기 용이하도록 안내문 등 부착
  - 설치장소에 표시가 곤란한 경우 구입물품 또는 그 포장에 그 장소를 표시 등
- 물류, 유통, 재고관리, 내부보안유지 등 내부 업무관리의 목적에 활용되어 일반 개인의 프라이버시 침해소지가 없는 경우에는 공공의 이익 또는 사업자의 편의 등을 고려하여 표시 의무 대상에서 제외하였다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.4	RFID태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○기관은 보안을 위해 기관 방문자에게 방문자의 이름,연락처, 소속기관 등의 개인정보가 담긴 RFID 카드를 발급하였고, 중요 시설공간에 리더기가 설치되어 있으나, 리더기 설치 사실을 안내하고 있지 않음.				

OO실 설치된 RFID 리더기	

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인

제10조(RFID 리더기 설치의 표시) 누구든지 RFID 태그가 부착 또는 내장되어 이용자에게 교부된 물품에 대한 정보 또는 RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우에는 리더기가 설치되어 있다는 사실을 이용자가 용이하게 인식할 수 있도록 표시하여야 한다. 다만, 물류유통·내부 보안유지·재고 관리를 목적으로 리더기를 설치하거나 고정된 장소에 설치되지 않아 설치장소를 용이하게 표시하기 힘든 경우에는 그러하지 아니 하다.

관련 문서

- RFID 프라이버시 보호 가이드라인 해설서 – 제4장 제10조

세부분야	RFID 태그 부착 및 제거				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.5	● **구입 및 제공받은 물품에 RFID태그가 내장 및 부착되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 구입 및 제공받은 물품에 RFID 태그가 내장 및 부착되어 있을 경우 부착위치, 기록정보 및 기능에 대해 표시내용이 적절하지 않은 경우				
평가근거 및 의견	● ○○도서관은 도서대여와 관련하여 회원증에 RFID 태그를 부착하여 회원의 개인정보 및 도서대여정보를 확인할 수 있도록 하고 있으며, 태그 부착사실 및 기록되는 정보 등을 안내하고 있으나 RFID 성질 및 기능, 개인정보관리책임자의 연락처는 안내하고 있지 않음				

주요 점검 사항

1. 구입 및 제공받은 물품에 RFID 태그가 내장 또는 부착되어 있는 경우에는 부착 위치, 기록정보 및 기능에 대하여 표시하도록 하여야 한다.

지표 해설

- 이용자가 물품을 구입하거나 제공받은 이후에도 당해 물품에 태그가 내장 또는 부착되어 있는 경우에 취급사업자는 이용자에게 RFID 활용과 관련한 일정한 사항을 설명하거나 표시하여 쉽게 알 수 있도록 하여야한다.
  - 이용자가 물품 구입 후 RFID 태그를 제거하지 않아 그 기능이 활성화되어 있는 경우에는 개인정보와의 연계 및 위치추적 등 개인정보 침해 우려가 있으므로 취급사업자에게 부착 사실 등에 대한 표시 의무를 부여한 것이다.
- 이용자로 하여금 RFID 태그가 부착되어 있다는 사실을 명확히 인식시켜 줌으로써 물품 구입 등의 사후에 이용자 스스로 자신의 행위에 대하여 결정내릴 수 있도록 하자는데 그 취지가 있다. 〈RFID 프라이버시 보호 가이드라인 해설서〉
  - 설명 방법 : 물품 구입시 백화점 매장 등에서 판매 직원이 직접 구두로 설명하거나, 판매대·출입구 등에 동 내용을 알기 쉽게 설명한 문구를 게시
  - 표시 방법 : 물품 또는 그 포장에 직접 인쇄 또는 물품 또는 포장에 고지사항이 포함된 라벨의 부착 등

설명 및 표시 내용
1. RFID 태그가 부착되어 있다는 사실 및 그 부착위치 - RFID 태그는 그 자체로 은밀하다는 속성을 지니고 있기 때문에 이용자의 인식 없이 물품 등에 RFID 태그를 얼마든지 탑재 또는 내장할 수 있다. - 따라서 이용자가 물품에 RFID 태그 부착 사실 및 그의 개인정보 침해 가능성을 인식하도록 하여 사전에 자신의 구매 의사를 결정할 수 있도록 하여야 한다. 2. RFID 태그의 성질 및 기능 - 이용자로 하여금 물품 등에 부착된 RFID 태그의 성질과 기능을 알 수 있도록 하여 해당 물품에 대한 구매 여부 결정 등 적절한 선택의 기회를 제공하여야 한다. 3. RFID 태그에 기록되어 있는 정보 - RFID 태그에 어떠한 정보가 기록되어 있는지에 대한 정보를 이용자에게 알려줌으로써 보다 해당 물품의 특성을 잘 이해하여 프라이버시 침해의 우려에 대한 판단할 수 있는 기준을 제시할 수 있다. 4. 제13조의 규정에 의한 개인정보 보호책임자의 연락처 등 - RFID 태그가 부착된 물품을 구입한 이후에 해당 태그로 인해 개인 정보침해 등 문제가 발생할 경우에 이용자가 용이하게 고충해결을 요구하고 해결할 수 있는 창구를 제공하여 이용자의 권리를 보호하여야 한다.

- RFID 태그의 부착사실에 대하여 물품 또는 그 포장에 설명 또는 표시가 곤란한 경우에는, 당해 물품을 판매하거나 용역을 제공하는 장소에 제1항 각호의 내용을 게시하여야 한다. 〈RFID 프라이버시 보호 가이드라인 해설서〉

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.5	구입 및 제공받은 물품에 RFID태그가 내장 및 부착 되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○도서관은 도서대여와 관련하여, 회원증에 RFID 태그를 부착하여 회원의 개인정보 및 도서대여정보를 확인할 수 있도록 하고 있으나, 태그 부착사실, 기록되는 정보, RFID 성질 및 기능, 개인정보관리책임자의 연락처 등 안내해야 할 사항에 대한 안내가 없음. RFID 태그부착 사실 미 안내 				

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제7조(RFID 태그 부착 사실 등의 표시) ① RFID 취급사업자는 이용자가 물품을 구입하거나 제공받은 이후에도 당해 물품에 RFID 태그가 내장 또는 부착되어 있는 경우에는 다음 각 호의 사항을 미리 이용자에게 설명하거나 당해 물품 또는 그 포장에 표시하여야 한다.

1. RFID 태그가 부착되어 있다는 사실 및 그 부착 위치
2. RFID 태그의 성질 및 기능
3. RFID 태그에 기록되어 있는 정보
4. 제13조의 규정에 의한 개인정보관리책임자의 연락처 등

② RFID 취급사업자는 제1항의 규정에 의한 설명 또는 표시가 곤란한 경우에는 당해 물품을 판매하거나 용역을 제공하는 장소에서 이용자가 쉽게 알아볼 수 있는 방법으로 제1항 각호의 사항을 게시하여야 한다.

관련 문서

- RFID 프라이버시 보호 가이드라인 해설서 – 제3장 제7조

세부분야	RFID 태그 부착 및 제거				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.6	● **RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그기능을 제거하는 방법 또는 수단을 제공하고 있지 않은 경우				
평가근거 및 의견	● ○○의료원에서는 환자관리를 위해 비상 시 필요한 의료정보, 과거 환자의 치료기록, 약물치료 등 의료기록 및 성명, 주소, 연락처 등 인적사항이 기록된 RFID 진료카드를 발급하였으나, 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하고 있지 않음				

주요 점검 사항

1. RFID 태그가 내장 또는 부착되어 있는 경우에는 판매 또는 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 하여야 한다.

지표 해설

● RFID 취급사업자는 이용자가 물품을 구입한 이후에도 당해 물품에 RFID 태그가 부착 또는 내장되어 그 기능이 계속 활성화 상태로 유지되도록 한 경우에는 그 사실을 이용자에게 알려주어 이용자가 원하는 경우에는 RFID 태그의 기능을 제거할 수 있도록 그 방법에 대하여 설명하거나 표시하여야 한다. 〈RFID 프라이버시 보호 가이드라인 해설서〉

※ RFID 태그의 기능이 활성화 상태로 유지된다는 것은 이용자가 물품을 구입한 이후에도 그 물품에 부착된 태그의 기능이 살아 있어 향후 언제든지 RFID 리더기에 의해 해당 태그의 내용이 판독될 수 있는 상태로 두는 것을 말한다.

기능 제거의 의미
- RFID 태그의 "기능을 제거한다"는 것은 RFID 태그를 물품 등에서 완전히 분리, 탈착하거나 또는 RFID 태그를 부착하였지만 그 기능을 차단(비활성화)하여 구입 물품과 태그와의 상관관계 및 연결고리를 단절되도록 하여 리더기로 판독이 불가능한 상태로 한다는 것을 말한다.

RFID 태그의 기능 제거 방법 예시
- RFID 태그 자체를 떼어냄 - 동전, 송곳 등 간단한 도구를 이용한 스크래칭 등 간단한 조작으로 전자적으로 태그 정보의 판독을 불가능하게 함 - 알루미늄 포장 등을 이용하여 RFID 태그의 내용을 리더기가 판독할 수 없도록 차단

- RFID 취급사업자는 이용자가 용이하게 해당 태그를 제거할 수 있도록 수단 또는 도구를 제공하여야 한다. 〈RFID 프라이버시 보호 가이드라인 해설서〉

RFID 태그 기능 제거 수단 제공의 예시
- 이용자에게 물품판매 시 태그를 간단히 분리하거나 기능을 비활성화 할 수 있는 장치 또는 도구와 함께 사용 설명서를 첨부하여 제공 ※ 조립제품 판매시 조립을 용이하게 할 수 있도록 간단한 도구를 첨부하여 판매하는 방법을 RFID 태그가 부착된 물품을 판매하는 경우에도 활용할 수 있을 것임

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.6	RFID태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 계획하고 있습니까?			○	
평가근거 및 의견	● ○○도서관은 도서대여와 관련하여, 회원의 개인정보 및 도서대여정보를 확인할 수 있도록 회원증에 RFID 태그를 부착하여 발급하고 있으나, 태그를 제거할 수 있는 방법에 관하여 회원증에 표기하거나 도서관에 게시하는 등 이용자에게 안내 및 제공을 하고 있지 않음. 				

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제8조(RFID 태그의 기능제거 방법 등에 대한 표시) ① RFID 취급사업자는 이용자가 물품을 구입하거나 제공받은 이후에도 당해 물품에 RFID 태그가 내장 또는 부착되어 있는 경우에는 이용자가 스스로 RFID 태그의 기능을 제거할 수 있는 방법 등을 설명하거나 해당 물품 또는 그 포장에 표시하여야 한다.

② RFID 취급사업자는 제1항의 규정에 의한 설명 또는 표시가 곤란한 경우에는 당해 물품을 판매하거나 용역을 제공하는 장소에서 이용자가 쉽게 알아볼 수 있는 방법으로 제1항 규정의 RFID 태그의 기능정지 방법 등을 게시하여야 한다.

③ RFID 취급사업자는 RFID 태그가 내장 또는 부착된 물품 등을 구입한 이용자가 용이하게 RFID 태그의 기능을 제거할 수 있는 수단을 제공하여야 한다.

④ RFID 취급사업자는 이용자가 RFID 태그를 제거하였다는 이유로 부당하게 이용자에게 불이익을 주거나 이용자를 차별하여서는 아니 된다.

⑤ RFID 취급사업자는 제1항 규정의 RFID 태그의 기능을 제거하는 것이 이용자의 이익이나 공공의 이익을 해칠 우려가 있는 경우에는 그 이유를 이용자에게 설명하거나 해당 물품 또는 그 포장에 표시하여야 한다.

관련 문서

- RFID 프라이버시 보호 가이드라인 해설서 – 제3장 제8조

세부분야	RFID 태그 부착 및 제거				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.2.7	● **이용자의 신체에 RFID를 지속적으로 착용하지 않도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : RFID를 지속적으로 착용하도록 계획하지 않은 경우(법률에 규정하는 경우 포함)				
평가근거 및 의견	● ○○청은 ○○법제○○조(○○명령의 집행)에 의해 범죄자로 하여금 사고재발방지를 위해 전자장치를 착용시키도록 하고 있음				

주요 점검 사항

1. 정보주체의 신체에 RFID를 지속적으로 착용하지 않도록 하여야 한다.

지표 해설

- RFID 태그가 인체에 이식되는 경우 개인의 위치가 파악될 수 있는 위험성이 있어, 단순히 사물에 부착하는 경우보다 개인정보 및 개인 프라이버시 침해 가능성이 매우 높다.
  - 따라서 누구든지 법률에 특별한 규정이 있는 경우를 제외하고는 RFID 태그의 인체 이식을 금지하였다.(현재로서는 인체이식에 대한 아무런 법률 규정이 없으므로, 관련 법률이 제정되기 이전에는 RFID 태그의 인체 이식은 금지된다)
  - 한편, 순수한 "연구 목적"으로 RFID 태그를 인체에 이식하는 경우에도 법률에 근거가 없으면 허용되지 않는다고 보아야 한다.

RFID 태그 "인체 이식"의 의미
- 인체의 일부분 어느 곳이든지 RFID 태그를 삽입하거나 붙이는 행위 또는 이와 유사한 일체의 행위를 말한다.

- 태그의 인체이식의 경우 법률에 의한 경우라도 가능한 한 장기간의 이식 상태는 제한되어야 하며 그 상태는 한시적·단발적으로 이루어져야 하는 것이 바람직하다.
- 또한 관련 법률에 따라 RFID 태그를 이식하는 경우에도 이식 대상자에게도 언제든지 당해 RFID 태그를 제거할 수 있도록 권한을 부여하여야 한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.2.7	이용자의 신체에 RFID를 지속적으로 착용하지 않도록 계획하고 있습니까?				○
평가근거 및 의견	● ○○청은 ○○법 제○○조(○○명령의 집행)에 의해 범죄자로 하여금 사고재발방지를 위해 전자장치를 착용시키도록 하고 있음.				

○○법 제○○조	**제7조(부착명령의 집행)** ① 보호관찰관은 피부착명령자에 대한 판결문 등본, 법 제12조제2항의 부착명령 집행을 지휘한 서면, 그 밖의 관련 서류를 확인한 후 부착명령을 집행하여야 한다. ② [redacted] 제13조제1항에 따라 부착명령을 집행하기에 앞서 [redacted]에 따른 피부착자의 의무사항 및 법 제38조 및 제39조에 따른 벌칙에 관한 사항을 알려야 한다. ③ 부착명령은 다음 각 호의 방법으로 집행한다. [redacted] **제11조(전자장치의 효용 유지 의무)** 피부착자는 전자장치의 부착기간 중 법 제14조제1항에 따라 전자장치의 효용 유지를 위하여 다음 각 호의 사항을 준수하여야 한다. 1. 전자장치의 기능이 정상적으로 유지될 수 있도록 전자장치를 충전, 휴대 또는 관리할 것 2. 전자장치가 정상적으로 작동하지 아니하는 경우 지체 없이 그 사실을 보호관찰관에게 알릴 것 3. 전자장치의 기능 유지를 위한 보호관찰관의 정당한 지시에 따를 것

관련법령 및 문서

관련 법령 · 지침

【RFID 프라이버시 보호 가이드라인】

제9조(RFID 태그의 인체이식 등 금지) ① 누구든지 RFID 태그를 인체에 이식하거나 제거할 수 있는 권한을 부여하지 아니하고 이용자의 신체에 RFID 태그를 지속적으로 착용하도록 하여서는 아니 된다. 다만, 법률에 특별한 규정이 있는 경우는 그러하지 아니하다.

② 누구든지 법률에 특별한 규정이 있는 경우를 제외하고는 RFID 태그를 이용자가 인식할 수 없는 방법으로 물품 등에 부착하여서는 아니 된다.

관련 문서

● RFID 프라이버시 보호 가이드라인 해설서 – 제3장 제9조

3 바이오 정보

세부분야	원본정보 보관 시 보호조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.3.1	● **수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?**			○	
평가 예시	● 미이행 : 바이오 원본정보와 제공자의 신상정보를 전부 혹은 일부에 대해 별도로 분리하여 관리하고 있지 않은 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 바이오 원본정보(홍채 정보)와 성명 등 신상정보를 별도로 분리하도록 계획하고 있음20XX.XX.XX 회의록을 확인한 바, 운영중인 홍채인식시스템에서 ○○○, YYY부서의 홍채정보는 신상정보와 분리하여 관리하고 있으나 XXX 부서의 홍채정보는 현재 분리하여 관리하고 있지 않고 향후 분리할 예정임				

주요 점검 사항

1. 바이오정보를 수집하는 경우에는 수집된 바이오정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)을 별도로 분리하여 저장하여야 한다.

지표 해설

- 바이오정보는 변경이 불가능하다는 특성으로 인해 유출 시 다른 정보에 비해 유출시 위험성이 매우 크기 때문에 안전한 관리에 더욱 주의해야 한다.
- 바이오정보와 원본정보와 그 제공자를 알 수 있는 정보를 함께 보관하는 경우 유출 시 프라이버시 침해의 정도가 크므로 분리하여 보관하여야 하며, 바이오정보는 수집 후 지체 없이 암호화하여 보관한다. (바이오정보는 「개인정보 보호법」에 따라 암호화 필수)
- 원본정보는 특정정보 생성 후 파기를 원칙으로 한다.
  - 단, 원본정보 보관에 대한 법적 근거나 제공자의 동의가 있는 경우에는 암호화 및 기타 보호조치를 취한 후 안전한 저장매체에 보관할 수 있다.
- 민감한 원본정보는 성명, 연락처, 주소 등 제공자를 알 수 있는 정보와 분리하여 별도의 저장장치에 보관하는 것을 원칙으로 한다.(물리적 분리)
  - 단, 이것이 여의치 않아 동일한 저장공간 내에 보관할 경우 별도 DB로 분리하여 침해위험을 최소화해야 한다.(논리적 분리)

- 이 때, 원본정보와 제공자를 알 수 있는 개인정보를 상호 연결하는 공통 식별자로는 사원번호 등 직접적으로 제공자를 나타내지 않는 정보를 사용하는 것이 좋다.

용어 설명

※ 바이오정보 : 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.3.1	수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?			○	
평가근거 및 의견	● △△△ 기관은 바이오 원본정보(홍채 정보)와 성명, 주민등록번호 등 신상정보를 별도로 분리하도록 계획하고 있음. 20XX.XX.XX 회의록을 확인한 바, 운영 중인 홍채인식시스템에서 ○○○, YYY부서의 안구정보는 신상정보와 분리하여 관리하고 있으나 XXX 부서의 안구정보는 현재 분리하여 관리하고 있지 않고 향후 분리할 예정임.				

회의록	회 의 록
	목 적: 개인정보보호 관련
	일 시: 201
	장 소: 회의실
	참석자(5인): 박
	회 의 내 용
	□ 회의 내용 1. 홍채인식 시스템 보완의 건 o 기존 홍채정보(안구 정보)와 신상정보의 별도 분리 작업 추진의 건 - OOO부 관리하는 홍채정보(안구 정보)는 신상정보와 별도 분리작업 완료 - YYY부 관리하는 홍채정보(안구 정보)는 신상정보와 별도 분리작업 완료 - : XXX부 관리하는 홍채정보(안구 정보)는 신상정보와 별도 분리작업 미 수행 => 다음 분기(9월) 수행 예정

관련법령 및 문서

관련 법령 · 지침

【바이오정보보호 가이드라인】

제5조(수집) ① 운영자는 바이오정보를 수집하는 경우 제공자의 동의를 얻어야 한다. 다만, 법령에서 달리 규정하는 경우에는 그러하지 아니하다.

② 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각 호의 사항을 제공자에게 알리고, 이를 충분히 설명하여야 한다.

1. 수집하고자 하는 바이오정보의 종류
2. 바이오정보의 수집목적 및 보유기간
3. 바이오정보의 구체적인 처리방법
4. 바이오정보관리책임자의 성명·소속부서·직위·연락처 등의 인적사항
5. 바이오정보의 수집, 고지한 수집목적외 이용이나 제3자제공에 대한 동의의 철회 또는 바이오정보의 열람, 이용내역의 조회나 오류정정의 요구 등 제공자의 권리 및 그 행사방법
6. 그 밖에 제공자의 권익을 보호하기 위하여 필요한 사항

③ 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에 법령에서 달리 규정하는 경우를 제외하고는 제공자가 만18세 미만인 자, 심신박약으로 인하여 한정치산 선고를 받은 자 또는 금치산 선고를 받은 자(이하 "만18세 미만인 자 등"이라 한다)인 때에는 제공자의 동의 외에 그의 법정대리인의 동의를 얻어야 한다. 이 경우 운영자는 제공자의 법정대리인에게 제2항의 규정에 의한 고지 및 설명을 하여야 한다.

④ 운영자는 제공자의 신체적·행동적 특징에 관한 원본정보에서 특징정보를 생성할 경우 수집 목적 상 필수 불가결한 정보만을 생성하도록 하여야 한다.

제6조(보관) 운영자는 수집한 원본정보를 보관하는 경우에는 성명·주민등록번호·주소 등 제공자를 알 수 있는 정보와 별도로 분리하여야 한다.

관련 문서

- 바이오정보 보호 가이드라인 해설서 – 6. 바이오정보의 보관

세부분야	원본정보 보관 시 보호조치				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.3.2	● **원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 계획하고 있습니까?**		○		
평가 예시	● 부분이행 : 특징정보 생성 후 원본정보를 복원할 수 없는 방법으로 파기하는 계획이 있으나 확인절차가 미흡한 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 바이오 원본정보(홍채 정보)의 특징정보를 생성한 후 지체없이 파기하도록 '개인정보보호지침'의 '제65조(바이오 정보의 파기)' 항목에 규정되어 있으나 파기 방법 및 파기 확인 절차는 수립되어 있지 않음				

주요 점검 사항

1. 바이오정보를 수집하는 경우 원본정보에 대해서는 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 하여야 한다.

지표 해설

- 바이오 정보의 보유가 불필요하게 된 경우에는 해당 개인정보파일을 지체 없이 파기하도록 한다. (제공자의 별도 동의나 법률 규정이 있는 경우 예외)
- 기본적으로 바이오 인식시스템을 통한 개인 식별은 특징정보의 비교를 통해 이루어지므로, 원본정보에서 특징정보가 생성되면 원본정보의 수집목적 등은 달성한 것으로 볼 수 있기 때문에 지체 없이 파기하도록 한다.

바이오정보의 파기 방법
· 보유한 바이오정보를 전부 파기하여야 하는 경우에는 초기화 또는 전체 겹쳐쓰기(Overwrite)를 한 후 물리적으로 파괴(Destroy)한다. · 특정 개인 또는 일부의 바이오정보를 파기하여야 하는 경우에는 겹쳐쓰기(Overwrite)를 한다.

- 운영자 또는 바이오정보를 제공받은 제3자가 제공자 또는 법정대리인의 수집, 수집목적 외의 이용, 제3자 제공의 동의철회에 따라 해당 바이오정보를 파기한 때에는 제공자 또는 그의 법정대리인에게 파기사실을 통지하여야 한다. 〈바이오정보 보호 가이드라인 해설서〉

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.3.2	원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 계획하고 있습니까?		○		
평가근거 및 의견	● △△△ 기관의 바이오 원본정보(홍채 정보)의 특징정보를 생성한 후 지체 없이 파기하도록 '개인정보 보호지침'의 '제65조(바이오 정보의 파기)' 항목에 규정되어 있으나 파기 방법 및 파기 확인 절차는 수립되어 있지 않음.				

개인정보 보호지침	**제65조(바이오 정보의 파기)** ① 개인정보보호책임자는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 때에는 지체 없이 보유하는 제공자의 바이오정보를 복원할 수 없도록 파기하여야 한다. 1. 바이오정보의 수집·이용 목적 또는 제공받은 목적을 달성하거나 달성할 수 없게 된 경우. 단, 제공자의 별도 동의나 법률의 규정이 없는 한 원본정보는 특징정보 생성시 수집목적 등을 달성한 것으로 본다. 2. 바이오정보의 보유기간이 만료한 경우 3. 제공자 또는 법정대리인이 바이오정보의 수집, 수집목적 외의 이용 또는 제3자 제공에 대한 동의를 철회한 경우 4. 기타 바이오정보의 보유가 더 이상 필요하지 않게 된 경우 ② 개인정보보호책임자는 규정에 의하여 바이오정보를 파기한 경우에는 제공자에게 그 사실을 알려야 한다. 다만, 제공자가 만18세 미만인 자 등인 경우에는 제공자 외에 그의 법정대리인에게 그 사실을 알려야 한다.

관련법령 및 문서

관련 법령 · 지침

【바이오정보 보호 가이드라인】

제9조(파기) ① 운영자 또는 바이오정보를 제공받은 제3자는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 때에는 지체 없이 보유하는 제공자의 바이오정보를 복원할 수 없도록 파기하여야 한다.

1. 바이오정보의 수집·이용 목적 또는 제공받은 목적을 달성하거나 달성할 수 없게 된 경우. 단, 제공자의 별도 동의나 법률의 규정이 없는 한 원본정보는 특징정보 생성시 수집목적 등을 달성한 것으로 본다.
2. 바이오정보의 보유기간이 만료한 경우
3. 제공자 또는 법정대리인이 제10조의 규정에 의하여 바이오정보의 수집, 수집목적 외의 이용 또는 제3자 제공에 대한 동의를 철회한 경우
4. 기타 바이오정보의 보유가 더 이상 필요하지 않게 된 경우

② 운영자는 제1항 제3호의 규정에 의하여 바이오정보를 파기한 경우에는 제공자에게 그 사실을 알려야 한다. 다만, 제공자가 만18세 미만인 자 등인 경우에는 제공자 외에 그의 법정대리인에게 그 사실을 알려야 한다.

관련 문서

- 바이오정보 보호 가이드라인 해설서 9. 바이오정보의 파기

4 위치정보 활용

세부분야	개인위치정보 수집 동의				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.4.1	● **개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 받는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 '개인정보보호지침'의 '제70조(개인위치정보의 수집 시 동의)' 항목에 개인위치정보 수집 시 동의를 받도록 규정하고 있고, '이용약관 제62조(개인위치정보 수집)' 항목에 위치정보 수집자의 상호, 주소, 전화번호, 서비스 내용과 수집항목, 수집목적, 보유기간, 수집 미 동의 시 불이익 등에 대하여 안내하고 있고 서비스 가입 시 이용약관 동의를 받고 있음				

주요 점검 사항

1. 개인위치정보를 수집하는 경우에는 정보주체 또는 위치정보 수집장치 소유자에 대해 관련 사항을 명시적으로 알리고 동의를 받아야 한다.
   ① 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처
   ② 개인위치정보주체 또는 법정대리인의 권리와 그 행사방법
   ③ 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용
   ④ 위치정보 수집사실 확인 자료의 보유근거 및 보유기간
   ⑤ 개인위치정보의 수집방법
2. 개인위치정보를 수집하는 경우에는 위치정보사업자 허가 또는 위치기반서비스사업자 신고 대상인지 사전에 검토하여 필요시 허가 또는 신고를 하여야 한다.

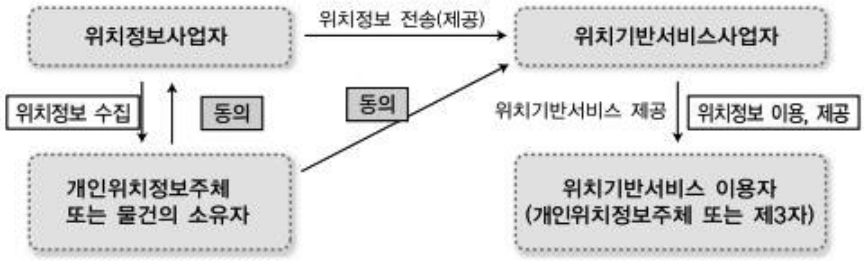
지표 해설

● 위치정보사업자는 개인위치정보주체가 개인위치정보 수집에 대한 각종 정보를 사전에 인지한 상태에서 개인위치정보 수집을 허용할지 여부를 결정할 수 있도록 하기 위해, 개인위치정보 수집 시 중요사항을 이용약관에 명시하고 동의를 받아야 한다.

이용약관 명시사항
· 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처 · 개인위치정보주체 및 법정대리인(14세 미만 아동의 경우)의 권리와 그 행사방법 · 위치기반서비스사업자가 제공하고자 하는 위치기반서비스의 내용 · 위치정보 이용·제공사실 확인 자료의 보유근거 및 보유기간 · 개인위치정보의 수집방법(시행령 제22조)

- 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 위치정보사업을 하고자 하는 자(위치정보사업자)는 방송통신위원회의 허가를 받아야 하며, 위치정보사업자로부터 위치정보를 제공받아 서비스를 제공하는 위치기반 서비스사업을 하고자 하는 자(위치기반서비스사업자)는 방송통신위원회에 신고를 하여야 한다.

위치정보사업과 위치기반서비스사업의 구분



※ 개인위치정보주체 또는 물건의 소유자와 위치기반서비스이용자는 동일인일 수 있음

용어 설명

※ "위치정보"라 함은 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하였거나 존재하였던 장소에 관한 정보로서 전기통신사업법 제2조제2호 및 제3호의 규정에 따른 전기통신설비 미 전기통신회선설비(RFID, GPS 등)를 이용하여 수집된 것을 말한다.

※ "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.4.1	개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?	○			
평가근거 및 의견	● △△△ 기관은 '개인정보 보호지침'의 '제70조(개인위치정보의 수집 시 동의)' 항목에 개인위치정보 수집시 동의를 받도록 규정하고 있고, '이용약관 제62조(개인위치정보의 수집)'항목에 위치정보수집자의 상호, 주소, 전화번호, 서비스 내용 등을 안내하고 있고 서비스 가입 시 이용약관 동의를 받고 있음.(수집항목, 수집목적, 보유기간, 동의 거부시 불이익 사항)				

개인정보 보호지침	**제70조(개인위치정보의 수집 시 동의)** ① 개인위치정보를 수집하고자 하는 경우에는 미리 다음 각호의 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다. 1. 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처 2. 개인위치정보주체 및 법정대리인(제25조제1항의 규정에 의하여 법정대리인의 동의를 얻어야 하는 경우에 한한다)의 권리와 그 행사방법 3. 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용 4. 위치정보 수집사실 확인자료의 보유근거 및 보유기간 5. 그 밖에 개인위치정보의 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항 ② 개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 수집의 범위 및 이용약관의 내용 중 일부에 대하여 동의를 유보할 수 있다. ③ 위치정보사업자가 개인위치정보를 수집하는 경우에는 수집목적을 달성하기 위하여 필요한 최소한의 정보를 수집하여야 한다.
이용 약관	제 62 조 (개인위치정보의 수집) 회사는 서비스를 제공하기 위하여 관련 법령의 규정에 따라 회원으로부터 필요한 개인정보를 수집합니다. 1. 위치정보사업자 상호 : ○○○(주) 주소 : 서울시 강남구 전화번호 : 02-XXX-XXXX 3. 개인위치정보에 기반한 ○○○정보 제공 4. 보유근거 : 정보주체 동의 5. 보유기간 : 서비스 가입기간
약관동의 화면	☑ **이용약관 동의** ○○ 서비스약관 (2009. 9. 6 부터 유효) 제1장 총 칙 제 1 조 (목적)

관련법령 및 문서

관련 법령 · 지침

【위치정보의 보호 및 이용 등에 관한 법률】

제5조 (위차정보사업의 허가등) ① 위치정보사업을 하고자 하는 자는 상호, 주된 사무소의 소재지, 위치정보사업의 종류 및 내용, 위치정보시스템을 포함한 사업용 주요 설비 등에 대하여 대통령령으로 정하는 바에 따라 방송통신위원회의 허가를 받아야 한다.

② 삭제 〈2009.3.13.〉

③ 방송통신위원회가 제1항의 규정에 의한 허가를 함에 있어서는 다음 각호의 사항을 종합적으로 심사하여야 한다.

1. 위치정보사업계획의 타당성
2. 개인위치정보 보호 관련 기술적·관리적 조치계획
3. 위치정보사업 관련 설비규모의 적정성
4. 재정 및 기술적 능력
5. 그 밖에 사업수행에 필요한 사항

④ 방송통신위원회는 제1항의 규정에 의하여 허가를 하는 경우에는 위치정보의 정확성·신뢰성 제고, 공정경쟁 또는 개인위치정보의 보호를 위한 연구·개발에 필요한 조건을 붙일 수 있다.

⑤ 제1항의 규정에 의한 허가의 대상자는 법인에 한한다.

⑥ 제1항의 규정에 의한 허가의 신청요령·절차 등에 관한 사항 및 제3항의 규정에 의한 심사사항별 세부심사기준은 대통령령으로 정한다.

⑦ 제1항에 따라 위치정보사업의 허가를 받은 자(이하 "위치정보사업자"라 한다)가 허가를 받은 사항 중 위치정보시스템을 변경(그 변경으로 개인위치정보 보호를 위한 기술적 수준이 허가받은 때보다 저하되는 경우에 한한다)하려는 경우에는 대통령령으로 정하는 바에 따라 방송통신위원회의 변경허가를 받아야 하고, 상호 또는 주된 사무소의 소재지를 변경하려는 경우에는 방송통신위원회에 변경신고를 하여야 한다.

⑧ 방송통신위원회는 제1항에 따른 허가 또는 제7항에 따른 변경허가의 신청이 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 허가 또는 변경허가를 하여야 한다.

1. 제3항에 따른 심사사항에 부적합한 경우
2. 신청한 자가 법인이 아닌 경우
3. 신청한 법인의 임원이 제6조제1항 각 호의 어느 하나에 해당하는 경우
4. 신청한 법인이 제13조제1항에 따른 허가 취소처분이나 사업의 폐지 명령을 받은 후 3년이 지나지 아니한 경우
5. 그 밖에 이 법 또는 다른 법률에 따른 제한에 위반되는 경우

제9조 (위치기반서비스사업의 신고) ① 위치기반서비스사업(개인위치정보를 대상으로 하지 아니하는 위치기반서비스사업은 제외한다. 이하 이 조, 제10조 및 제11조에서 같다)을 하고자 하는 자는 상호, 주된 사무소의 소재지, 사업의 종류, 위치정보시스템을 포함한 사업용 주요 설비 등에 대하여 대통령령으로 정하는 바에 따라 방송통신위원회에 신고하여야 한다.

② 제13조제1항의 규정에 의한 사업의 폐지명령을 받은 후 1년이 경과하지 아니한 자(법인인 경우에는 그 대표자를 포함한다)는 제1항의 규정에 의한 사업의 신고를 할 수 없다.

③ 제1항에 따라 위치기반서비스사업의 신고를 한 자(이하 "위치기반서비스사업자"라 한다)가 그 신고한 사항 중

상호, 주된 사무소의 소재지 또는 위치정보시스템을 변경(변경으로 인하여 개인위치정보 보호를 위한 기술적 수준이 신고한 때보다 저하되는 경우에 한한다)하고자 하는 때에는 대통령령이 정하는 바에 따라 방송통신위원회에 변경 신고를 하여야 한다.

④ 위치정보사업자가 제5조제1항에 따른 허가를 신청할 당시 위치기반서비스사업의 신고에 필요한 서류를 첨부한 경우에는 제1항에 따른 위치기반서비스사업의 신고를 한 것으로 본다.

제15조 (위치정보의 수집 등의 금지) ① 누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 제29조제1항에 따른 긴급구조기관의 긴급구조요청 또는 같은 조 제7항에 따른 경보발송 요청이 있는 경우
2. 제29조제2항에 따른 경찰관서의 요청이 있는 경우
3. 다른 법률에 특별한 규정이 있는 경우

② 누구든지 타인의 정보통신기기를 복제하거나 정보를 도용하는 등의 방법으로 위치정보사업자등을 속여 타인의 개인위치정보를 제공받아서는 아니된다.

③ 위치정보를 수집할 수 있는 장치가 부착된 물건을 대여하는 자는 위치정보 수집장치가 부착된 사실을 대여받는 자에게 고지하여야 한다.

제18조 (개인 위치정보의 수집) ① 위치정보사업자가 개인위치정보를 수집하고자 하는 경우에는 미리 다음 각호의 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다.

1. 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처
2. 개인위치정보주체 및 법정대리인(제25조제1항의 규정에 의하여 법정대리인의 동의를 얻어야 하는 경우에 한한다)의 권리와 그 행사방법
3. 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용
4. 위치정보 수집사실 확인자료의 보유근거 및 보유기간
5. 그 밖에 개인위치정보의 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

② 개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 수집의 범위 및 이용약관의 내용 중 일부에 대하여 동의를 유보할 수 있다.

③ 위치정보사업자가 개인위치정보를 수집하는 경우에는 수집목적을 달성하기 위하여 필요한 최소한의 정보를 수집하여야 한다.

【위치정보의 보호 및 이용 등에 관한 법률 시행령】

제22조 (위치정보 수집 시 이용약관 명시사항) 법 제18조제1항제5호에서 '대통령령이 정하는 사항"이란 개인위치정보의 수집방법을 말한다.

관련 문서

- 위치정보의 보호 및 이용 등에 관한 법률 해설서 – 4. 개인위치정보 수집 시 동의

세부분야	개인위치정보 제공 시 안내사항				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
5.4.2	● **개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치 정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하도록 계획하고 있습니까?**	○			
평가 예시	● 이행 : 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하는 경우				
평가근거 및 의견	● 평가대상기관인 △△△ 기관은 제3자인 ○○○서비스(주)에 개인위치정보를 제공하고 있으며 제공하는 경우 매회 제공받는 자, 제공일시, 제공목적을 SMS를 통해 통보하고 있으며, 개인위치정보 제공 현황 및 개인위치정보 통보 현황을 확인함				

주요 점검 사항

1. 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치정보주체에게 아래의 정보제공내역을 개인위치정보를 수집한 해당 통신단말장치 또는 개인위치정보주체가 미리 특정하여 지정한 통신단말장치 또는 전자우편주소로 통보하여야 한다.
   ① 개인위치정보를 제공받는 자
   ② 제공일시 및 제공목적
2. 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 정보제공내역을 매회 즉시 통보하여야 한다. 다만, 개인위치정보주체의 동의를 받은 경우에는 최대 30일의 범위에서 아래의 기준에 따라 정보제공내역을 모아서 통보할 수 있다.
   ① 횟수 : 10회, 20회 또는 30회 등 10배수의 횟수
   ② 기간 : 10일, 20일 또는 30일

지표 해설

● 개인위치정보는 위치정보사업자로부터 위치기반서비스사업자로 전송되어 이용·제공되므로, 위치기반서비스사업자가 개인위치정보를 이용·제공하는 경우에는 위치정보사업자가 수집 시 동의 받은 것과는 별도로 동의를 받는 절차가 필요하다.

위치정보 제3자 제공 동의 시 고지 사항(위치정보보호법 제19조)
1. 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처 2. 개인위치정보주체 및 법정대리인(법정대리인의 동의를 얻어야 하는 경우에 한함)의 권리와 그 행사방법 3. 위치기반서비스사업자가 제공하고자 하는 위치기반서비스의 내용 4. 위치정보 이용·제공사실 확인 자료의 보유근거 및 보유기간

- 개인위치정보를 제3자에게 제공하는 서비스는 단순 이용하는 것보다 개인프라이버시 침해의 위험이 높으므로 더욱 두텁게 보호할 필요성이 있는 바, 위치정보법은 이를 위해 사전 고지 및 동의와 사후 통보의무를 함께 규정하고 있다.
- 위치기반서비스사업자의 개인위치정보 제3자 제공에 대해서는 사전 동의의무가 부과되고, 사후적으로는 통보의무가 부과된다. 즉, 위치기반서비스사업자는 개인위치정보주체의 동의를 얻어 그가 지정하는 제3자에게 개인위치정보를 제공하는 경우에도 매회 개인위치정보를 제공받은 제3자, 제공일시, 제공목적을 개인위치정보주체에게 즉시 통보하여야 한다.

제3자 제공 시 통보방법(시행령 제24조)
· 원칙 : 위치정보사업자가 개인위치 정보를 수집한 당해 단말장치를 통해 통보 · 예외 : 미리 개인위치정보주체가 지정한 다른 통신단말장치나 전자우편주소로 통보 ① 개인위치정보를 수집한 당해 통신단말장치가 문자, 음성 또는 영상수신기능을 갖추지 아니한 경우 ② 개인위치정보주체가 다른 통신단말장치 또는 전자우편주소 등으로 통보할 것을 미리 요청한 경우

- 단, 개인위치정보 제3자 제공 동의를 받을 때 제3자에 대한 정보제공내역을 즉시 통보받는 방법과 모아서 통보받는 방법 중 선택하여 통보받을 수 있음을 고지하고 동의를 받을 수 있다. 이때 모아서 통보받는 방법은 최대 30일 범위에서 아래와 같이 횟수 및 기간 등의 기준을 정하여 시행할 수 있다.

제3자 제공 시 모아서 통보하는 기준
· 횟수 : 10회, 20회 또는 30회 등 10배수의 횟수 · 기간 : 10일, 20일 또는 30일 ※ 위의 횟수 및 기간 기준에 따라 모아서 통보하는 경우에는 최초로 제3자에게 개인위치정보를 제공한 날부터 30일이 될 때마다 다음 사항에 해당하는 정보제공내역을 모아서 통보해야 함 - 횟수 기준에 따라 모아서 통보한 후 남은 정보제공내역 - 제3자에게 개인위치정보를 제공한 횟수가 동의한 횟수에 이르지 아니하여 통보하지 아니한 정보제공내역

평가 예시

구 분	질의문	이행	부분이행	미이행	해당없음
5.4.2	개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하도록 계획하고 있습니까?	○			
평가근거 및 의견	● △△△ 기관은 제3자인 ○○○서비스(주)에 개인위치정보를 제공하고 있으며 제공하는 경우 매회 제공받는 자, 제공일시, 제공목적을 SMS를 통해 통보하고 있음. 개인위치정보 제공 현황 및 개인위치정보 통보 현황을 확인함.				

위치정보 통보현황

위치정보 통보 현황

연번	제공정보	제공받는 자	제공일시	제공목적
1	개인 위치정보	OOO서비스(주)	2014.03.31	OOO 서비스 제공
2	개인 위치정보	OOO서비스(주)	2014.04.3	OOO 서비스 제공
3	개인 위치정보	XXX서비스(주)	2014.04.3	XXX 서비스 제공
4				
5				
6				
7				
8				
9				

관련법령 및 문서

관련 법령 · 지침

【위치정보의 보호 및 이용 등에 관한 법률】

제19조 (개인위치정보의 이용 또는 제공) ① 위치기반서비스사업자가 개인위치정보를 이용하여 서비스를 제공하고자 하는 경우에는 미리 다음 각호의 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다.

1. 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처
2. 개인위치정보주체 및 법정대리인(제25조제1항의 규정에 의하여 법정대리인의 동의를 얻어야 하는 경우에 한한다)의 권리와 그 행사방법
3. 위치기반서비스사업자가 제공하고자 하는 위치기반서비스의 내용
4. 위치정보 이용·제공사실 확인자료의 보유근거 및 보유기간
5. 그 밖에 개인위치정보의 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

② 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 서비스를 하고자 하는 경우에는 제1항 각호의 내용을 이용약관에 명시한 후 제공받는 자 및 제공목적을 개인위치정보주체에게 고지하고 동의를 얻어야 한다.

③ 제2항의 규정에 의하여 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하여야 한다.

④ 위치기반서비스사업자는 제3항에도 불구하고 대통령령으로 정하는 바에 따라 개인위치정보주체의 동의를 받은 경우에는 최대 30일의 범위에서 대통령령으로 정하는 횟수 또는 기간 등의 기준에 따라 모아서 통보할 수 있다. 〈신설 2015.2.3.〉

⑤ 개인위치정보주체는 제1항·제2항 및 제4항에 따른 동의를 하는 경우 개인위치정보의 이용·제공목적, 제공받는 자의 범위 및 위치기반서비스의 일부와 개인위치정보주체에 대한 통보방법에 대하여 동의를 유보할 수 있다. 〈개정 2015.2.3.〉

제21조(개인위치정보 등의 이용 · 제공의 제한 등) 위치정보사업자등은 개인위치정보주체의 동의가 있거나 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인위치정보 또는 위치정보 수집·이용·제공사실 확인자료를 제18조제1항 및 제19조제1항·제2항에 의하여 이용약관에 명시 또는 고지한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니된다. 〈개정 2015.2.3.〉

1. 위치정보 및 위치기반서비스 등의 제공에 따른 요금정산을 위하여 위치정보 수집·이용·제공 사실 확인자료가 필요한 경우
2. 통계작성, 학술연구 또는 시장조사를 위하여 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우

【위치정보의 보호 및 이용 등에 관한 법률 시행령】

제23조(개인위치정보 이용·제공 시의 이용약관 명시사항) 법 제19조제1항제5호에서 "대통령령이 정하는 사항"이란 법 제19조제3항에 따른 통보에 관한 사항을 말한다.

제24조(개인위치정보 제공사실의 통보) ① 위치기반서비스사업자가 법 제19조제3항 및 제4항에 따라 개인위치정보주체에게 개인위치정보를 제공받는 자, 제공일시 및 제공목적(이하 이 조에서 "정보제공내역"이라 한다)을 통보하는 경우에는 위치정보사업자가 개인위치정보를 수집한 해당 통신단말장치로 통보하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인위치정보주체가 미리 특정하여 지정한 통신단말장치 또는 전자우편주소 등으로 통보할 수 있다.

1. 개인위치정보를 수집한 해당 통신단말장치가 문자, 음성 또는 영상의 수신기능을 갖추지 아니한 경우
2. 개인위치정보주체가 개인위치정보를 수집한 해당 통신단말장치 외의 통신단말장치 또는 전자우편주소 등으로 통보할 것을 미리 요청한 경우

② 위치기반서비스사업자가 법 제19조제4항에 따라 개인위치정보주체의 동의를 받으려는 경우에는 제3자에 대한 정보제공내역을 즉시 통보받는 방법과 모아서 통보받는 방법 중 선택하여 통보받을 수 있음을 고지하여야 한다. 〈신설 2015.8.3〉

③ 위치기반서비스사업자는 제2항에 따른 고지를 한 후 다음 각 호의 내용에 대하여 개인위치정보주체의 동의를 받아야 한다. 이 경우 위치기반서비스사업자는 법 제19조제2항에 따른 동의와 구별하여 별도로 동의를 받아야 한다. 〈신설 2015.8.3〉

1. 제4항에 따라 정보제공내역을 모아서 통보하는 횟수 또는 기간
2. 개인위치정보주체의 요청이 있는 경우에는 법 제19조제3항에 따른 즉시 통보 방법으로 변경할 수 있다는 사실 및 그 요청 방법

④ 위치기반서비스사업자는 법 제19조제4항에 따라 다음 각 호의 횟수 또는 기간마다 제3자에 대한 정보제공내역을 모아서 통보할 수 있다. 〈신설 2015.8.3〉

1. 횟수: 10회, 20회 또는 30회 등 10배수의 횟수
2. 기간: 10일, 20일 또는 30일

⑤ 위치기반서비스사업자가 제4항제1호에 따른 방법으로 통보하는 경우 최초로 제3자에게 개인위치정보를 제공한 날부터 30일이 될 때마다 다음 각 호에 해당하는 정보제공내역을 모아서 통보하여야 한다. 〈신설 2015.8.3〉

1. 제4항제1호에 따라 모아서 통보한 후 남은 정보제공내역
2. 제3자에게 개인위치정보를 제공한 횟수가 제4항제1호에 따라 동의한 횟수에 이르지 아니하여 통보하지 아니한 정보제공내역

관련 문서

- 위치정보의 보호 및 이용 등에 관한 법률 해설서 – 5. 개인위치정보 이용·제공 시 동의

개인정보 영향평가 FAQ

개인정보 영향평가 FAQ

FAQ 01 영향평가 수행 시점

Q 신규 정보화사업 구축사업과 관련하여 구축 시점에는 개인정보수가 100만건을 넘지 않으나 향후 100만명이 넘을 것이 확실한 경우, 언제 영향평가를 받아야 하는가?

A 현재 시점 기준으로는 개인정보 영향평가 대상은 아니지만, 개인정보의 증가에 따라 가까운 시기(1년 이내)에 「개인정보 보호법 시행령」 제35조의 기준을 초과할 것이 확실한 경우 개인정보 침해의 사전 예방을 위해 가급적 신규 정보화사업 구축 시점에 개인정보 영향평가를 수행할 것으로 권고합니다.

FAQ 02 영향평가 수행 대상

Q 30만명의 개인정보를 보유하고 있는 ○○○시스템은 100만명의 개인정보를 보유하고 있는 △△△시스템과 연계가 되어, ○○○시스템의 개인정보 처리화면에서 △△△시스템에서 보유하고 있는 개인정보를 조회, 변경, 삭제 가능하도록 구현되어 있습니다. 하지만 ○○○시스템에서 자체적으로 보유하고 있는 30만명 이외의 추가적인 정보주체에 대한 개인정보는 조회를 하거나 변경·삭제할 수 없도록 제한이 되어 있습니다. 이 경우 ○○○시스템은 영향평가 의무 대상이 되나요?

A 「개인정보 보호법 시행령」 제35조에 따르면 다른 개인정보파일과 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일은 영향평가 의무대상이 됩니다. 위의 경우 30만명 이외의 개인정보는 조회, 변경, 삭제가 불가능하므로 연계 결과 최대 정보주체수는 30만명으로 볼 수 있겠습니다. 따라서 ○○○시스템은 영향평가 의무 대상에서 제외가 가능할 것으로 판단됩니다.
다만, 연계방식이나 시스템 구성방식 등에 따라 연계되는 개인정보의 수가 달라질 수 있으므로 충분한 검토 후 의무 대상 여부를 판단할 필요가 있겠습니다.

FAQ 03 영향평가 수행 대상

Q 100만건이 넘는 개인정보가 종이문서로 존재하고, 정보시스템 상에는 5만건이 안된다면 영향평가 대상이 되나요?

A 영향평가의 대상은 「개인정보 보호법 시행령」 제35조(개인정보 영향평가의 대상)에 따라서 전자적으로 처리할 수 있는 개인정보파일에 한합니다. 따라서 종이문서는 100만건이라 할지라도 영향평가의 대상이 아닙니다.

FAQ 04 영향평가 대상

Q 사립대학교입니다. 개인정보 영향평가를 의무적으로 수행해야 하나요?

A 사립대학교의 경우에도 「개인정보 보호법」 제2조제6호 및 동법 시행령 제2조 (공공기관의 범위)에 따른 공공기관에 해당됩니다. 따라서 「개인정보 보호법」 제33조(개인정보 영향평가)에 따라서 개인정보 영향평가를 의무적으로 수행해야 합니다.

FAQ 05 영향평가 수행 대상

Q 공공기관의 내부망에 저장된 인사정보도 영향평가 대상이 되나요?

A 영향평가의 예외가 되는 개인정보파일은 따로 없습니다. 따라서 인사정보도 「개인정보 보호법 시행령」 제35조의 기준에 부합할 경우 영향평가 대상이 됩니다.

FAQ 06 영향평가 수행 주체

Q 중앙부처가 개발하고 지자체 등에 시스템을 배포하여 공통적으로 사용하는 국가보급 표준시스템에 대하여 개별 지자체에서 각각 영향평가를 수행해야 하나요?

A 원칙적으로 개인정보파일에 대한 관리 책임을 가지고 있는 기관에서 영향평가를 수행하여야 합니다. 즉 응용프로그램을 중앙부처가 개발·보급하였다 하더라도 물리적인 장비 및 개인정보파일이 지자체에 위치하는 경우 지자체가 영향평가 수행의 주체가 됩니다.

다만, 중앙부처에서 국가보급 표준시스템에 대한 영향평가를 이미 수행한 경우에는 해당 국가보급 표준시스템의 응용프로그램 부분을 제외한 나머지 평가지표(대상기관의 개인정보보호 관리체계, 대상시스템 개인정보보호 관리체계, 기술적 보호조치 중 응용프로그램 외에 서버, 네트워크 등 인프라와 관련된 지표 등)에 대해서만 영향평가를 수행하시면 됩니다. 이때, 제외 가능한 평가지표는 해당 국가보급 표준시스템의 성격, 구성 및 운영 방식, 중앙부처에 영향평가를 수행한 범위 등에 따라 상이할 수 있으므로, 중앙부처 및 영향평가 기관과 사전에 협의를 거쳐 제외항목을 결정할 것을 권고합니다.

FAQ 07 영향평가 사업 발주

Q 동일 기관 내에 다양한 부서에서 개인정보파일과 개인정보처리시스템을 개별적으로 운영하고 있습니다. 개인정보 영향평가를 각각 수행해야 하나요?

A 각각의 개인정보파일 및 개인정보처리시스템별로 영향평가를 수행할 수도 있고, 통합하여 수행할 수도 있습니다. 통합하여 발주시 영향평가 사업 수행의 효율성 측면에서 장점이 있으므로 통합하여 발주하는 방식을 권고합니다.

FAQ 08 영향평가 사업 발주

Q 발주기관에서 SI사업의 일환으로 영향평가를 포함하여 통합 발주하는 것이 가능한지요?

A 영향평가 사업을 SI사업에 포함하여 통합 발주할 경우, 영향평가 사업의 객관성과 독립성을 훼손할 가능성이 크므로, 분리 발주할 것을 권고합니다.

FAQ 09 영향평가 사업 발주

Q 영향평가 사업 발주 방식은 어떻게 해야 하나요?
반드시 협상에 의한 계약으로 해야 하는 건가요?

A 사업 발주 방식에 대해서는 별도의 권장 사항이 있지 않습니다.
기관의 편의에 따라 사업을 발주하시면 됩니다.

FAQ 10 영향평가 수행

Q 수행안내서에서 제시된 85개 평가항목은 반드시 그대로 사용해야 하나요?

A 최신 침해사례, 법 제도의 변화, 대상기관 및 대상 사업의 특성에 따라 추가, 삭제, 변경 등 탄력적으로 구성하여 사용 가능합니다. 예를 들어 「개인정보 보호법」외에 대상기관이 적용받는 법률에 개인정보 보호와 관련된 특별한 조항이 포함되어 있다면 평가항목에 추가하여 점검을 수행하는 것이 바람직합니다.
또한 「개인정보 보호법」 또는 관련 고시 등의 개정에 따라 기존 85개 평가항목과 상이한 사항이 발생할 수 있습니다. 따라서 영향평가 수행 시점에서 최신의 법률 등을 반드시 확인하여 평가항목의 추가·변경 필요성을 검토할 필요가 있습니다.

FAQ 11 영향평가 수행

Q 개인정보 위험도 산정 방식은 수행안내서에서 제시된 방법만 사용해야 하나요?

A 아닙니다. 영향평가 기관 고유의 위험 분석 방법론이 있다면 해당 방법론을 사용하여 위험도를 산정할 수 있습니다. 이 경우, 위험도 산정 과정 및 결과는 합리적이고 납득 가능해야 하며 위험도 산정값은 실질적인 위험의 크기를 대변할 수 있어야 합니다. 또한, 법적 준거성 등 개인정보보호 영역의 특성이 반영되어 있어야 합니다.

FAQ 12 영향평가 수행

Q 개인정보 흐름표, 개인정보 흐름도 등과 같이 수행안내서에 제시된 양식은 그대로 사용해야 하나요?

A 수행안내서에 제시된 양식은 예시일 뿐 반드시 그대로 사용할 필요는 없습니다. 영향평가 기관의 자체 방법론에 따라 대상 사업의 특성 등을 고려하여 양식을 추가 또는 일부 변형하여 사용할 수 있습니다. 이 경우 수행안내서에 제시된 영향평가 각 단계별 기본 절차는 준수하여야 하며, 영향평가 품질 측면에서 각 절차의 취지 및 목적을 달성할 수 있도록 하여야 합니다.

FAQ 13 영향평가 수행

Q 개인정보 영향평가 결과 도출된 침해요인은 모두 조치되어야 하나요?

A 도출된 침해요인은 모두 조치하는 것이 원칙이지만, 위험분석의 결과 위험도가 아주 낮거나 하는 등 합리적인 사유로 조치할 필요가 없다고 판단된다면 기관 내부의 의사결정 절차를 거쳐 조치하지 아니할 수 있습니다. 다만 법적 필수 사항인 경우에는 모두 조치될 수 있도록 하여야 합니다.

FAQ 14 영향평가 수행

Q 정보화 사업 범위에 고유식별정보에 대한 DB암호화가 포함되어 있습니다. 행정안전부 "개인정보 위험도 분석기준"에 따라 내부망 고유식별정보 DB암호화 여부를 판단하기 위한 위험도 분석을 수행하여야 하나요?

A 내부망에 저장되는 고유식별정보에 대하여 DB암호화를 적용하는 것이 사업 범위에 이미 포함되어 있다면 "개인정보 위험도 분석기준"에 따른 위험도 분석은 별도로 수행할 필요가 없습니다.

FAQ 15 영향평가 수행

Q 「개인정보의 안전성 확보조치 기준 고시」 제7조제4항에 따르면 내부망에 고유식별정보를 저장할 경우 위험도 분석이나 영향평가의 결과에 따라 암호화 여부를 결정할 수 있다고 되어 있는데, 영향평가 시 관련 지표가 따로 있나요?

A 영향평가의 경우에는 고유식별정보의 내부망 저장 시 암호화 여부를 결정하기 위해서 "개인정보 위험도 분석기준"의 26개 체크리스트를 준용하도록 권고하고 있습니다. 결국 영향평가 시에도 내부망에 저장된 고유식별정보의 암호화 여부를 판단하기 위해서는 "개인정보 위험도 분석기준"에 따른 위험도 분석을 수행하게 됩니다.(영향평가 지표 4.3.1 참고)

단, 위의 고유식별정보는 '주민등록번호를 제외한 고유식별정보'를 의미합니다.

주민등록번호는 「개인정보 보호법 시행령」 제21조의2(주민등록번호 암호화 적용 대상 등)에 따라 저장 위치와 상관없이 의무적으로 암호화를 하셔야 합니다.

FAQ 16 영향평가 수행

Q 다수의 개인정보파일 및 개인정보처리시스템에 대한 영향평가 사업을 통합 발주한 경우 영향평가서는 어떻게 작성해야 하나요?

A 영향평가서는 개인정보처리시스템별로 각각 작성하는 것을 권고드립니다. 예를 들어 5개의 개인정보처리시스템에 대하여 동시에 영향평가를 수행하였다면 5개의 영향평가서를 작성하시면 됩니다. 다만 "대상기관 개인정보보호 관리체계" 평가 영역은 중복되게 되므로 하나의 영향평가서에만 포함하시면 됩니다.

FAQ 17 영향평가서 제출

Q 영향평가 수행 후 영향평가서를 제출하는 방법은 어떻게 되나요?

A 개인정보보호 종합지원시스템(http://intra.privacy.go.kr)의 영향평가 메뉴에서 영향평가서를 등록하시면 됩니다.

FAQ 18 영향평가서 제출

Q 개인정보 영향평가를 수행한 후에 영향평가서를 언제까지 보호위원회에 제출하여야 하나요?

A 공공기관의 장은 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축·운용하기 전에 그 영향평가서를 보호위원회에 제출하여야 합니다. 다만, 기존에 운용 중이던 개인정보파일인 경우에는 영향평가서를 제출받은 날로부터 2개월 이내에 영향평가서를 보호위원회에 제출하여야 합니다.

FAQ 19 개선사항 이행확인서 제출

Q 영향평가 이행점검 결과는 언제까지 어떻게 제출해야 하나요? 또한 미완료된 건에 대해서는 어떻게 처리해야 하나요?

A 영향평가 사업을 통해 영향평가서를 제출받은 날로부터 1년 이내에 개인정보보호 종합지원시스템(http://intra.privacy.go.kr)의 영향평가 메뉴에서 "개선사항 이행확인서"를 등록하시면 됩니다.
모든 개선계획이 반드시 1년 이내에 완료될 필요는 없으며, 예산 등이 수반되어 1년 이내에 조치완료가 어려운 개선과제에 대해서는 이행점검 시점의 현황 및 계획을 작성해 주시면 됩니다.
※ 「개인정보 영향평가에 관한 고시」 제14조(영향평가 개선사항 이행) 참조