「개인정보 보호법」에 따른

개인정보 영향평가(PIA)

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다.

Privacy by Trust, Trust by Privacy

※ 저작권 등의 문제로 본 교재의 외부 공개를 금지합니다.

주요안내

본 교육자료는 「개인정보 보호법」 제33조 및 「개인정보 보호법 시행령」 제35조에서 규정한 내용을 기초로 합니다.

Contents

Ⅰ 개인정보 영향평가 제도 소개

Ⅱ 영향 평가 수행절차

Ⅲ 개인정보 처리 단계별 요구사항

Contents

Ⅰ 개인정보 영향평가 제도 소개

1. 개인정보 영향평가 개요

2. 용어정의 및 추진근거

3. 개인정보 영향평가 수행절차 요약

1 개인정보 영향평가 제도 소개

1.1. 개인정보 영향평가 개요

개 념

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

목적 및 필요성

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

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)** 영 제35조에 근거하여 영향평가를 실시한 기관이 개인정보 검색체계 등 개인정보파일의 운용체계 를 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

개인정보 영향평가를 하지 아니하거나 그 결과를 보호위원회에 제출하지 아니한 자에게는 개인정보 보호법 시행령 제75조 제2항16호에 근거하여 3천만원 이하의 과태료를 부과함('24.3.15.시행)

개인정보파일 및 개인정보처리시스템 정의

개인정보파일

(정의) 개인정보파일은 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인 정보의 집합물(集合物)을 말한다. 개인정보파일은 데이터베이스 등 전자적인 형태뿐만 아니라 수기(手記)문서 자료 도 포함하지만, 영향평가의 대상이 되는 개인정보파일은 전자적으로 처리할 수 있는 것에 한정되어 있으므로 일반 적으로 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 데이터베이스시스템 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, 개인 정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있으 며 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 및 시행령 제2조)

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」

1의2.「고위공직자범죄수사처 설치 및 운영에 관한 법률 제3조제1항에 따른 고위공직자범죄수사처」

2.「공공기관의 운영에 관한 법률 제4조에 따른 공공기관」

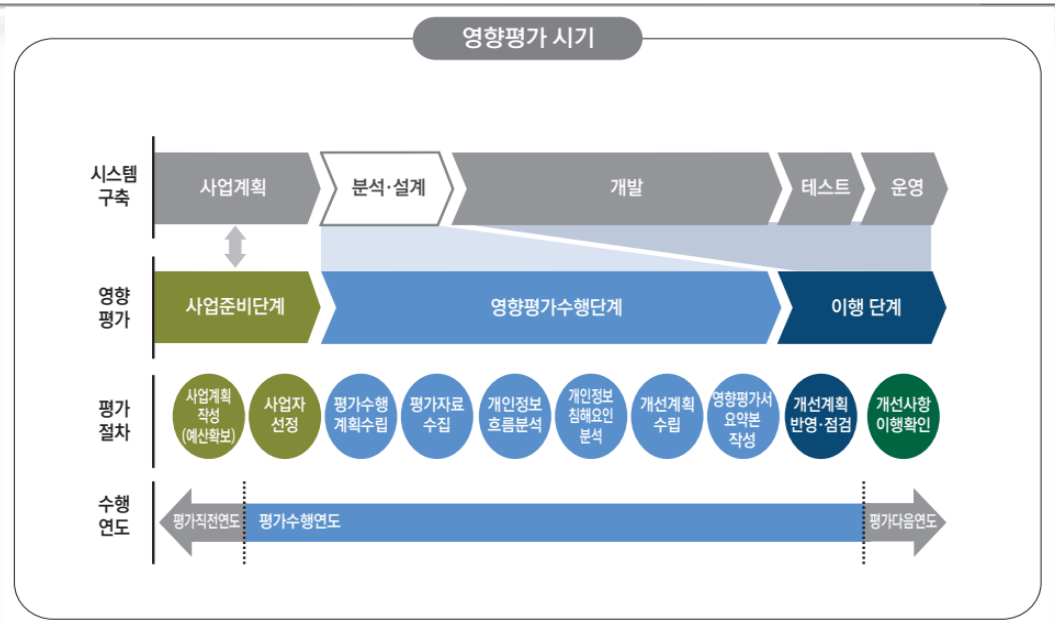
3.「지방공기업법 에 따른 지방공사 및 지방공단」

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, 대법원 규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따름 (「개인정보 보호법 제33조 제10항)

평가 시기



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)

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

평가 수행 주체

공공기관은 개인정보보호위원회가 지정한 영향평가기관에 평가를 의뢰하여 수행

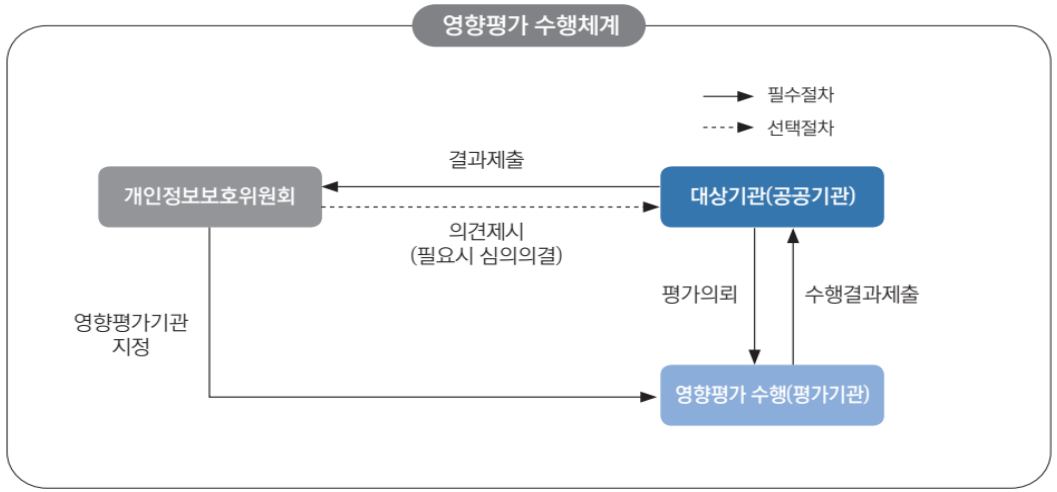
※ 영향평가기관에 대한 정보는 개인정보 포털(privacy.go.kr)에서 확인 가능소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체

평가 수행 체계

영향평가는 개인정보보호위원회가 지정한 영향평가기관에 의뢰하여 영향평가를 수행하고 그 결과 및 요약 본을 최종 제출받은 날로부터 2개월 이내에 개인정보보호위원회에 제출*

- 개인정보보호위원회는 필요 시 영향평가 결과에 대한 의견 제시 가능

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



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 정보 와 쉽게 결합하여 개인을 알아볼 수 있는 정보가 포함됨. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려해야 함. 또한 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 가명처리한 정보 즉, 가명정보도 개인정보에 포함 (「개인정보 보호법」 제2조제1호)
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 개인 정보의 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)
고정형 영상정보 처리기기	일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유· 무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치(「개인정보 보호법」 제2조제7호)
이동형 영상정보 처리기기	사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치(「개인정보 보호법」 제2조제7의2)
민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서, 유전자검사 등의 결과로 얻어진 유전정보, 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보 (「개인정보 보호법」 제23조제1항 및 동법 시행령 제18조)

용어정의

고유식별정보	법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 의미(「개인정보 보호법」 제24조제1항 및 동법 시행령 제19조)
개인정보취급자	개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말함(개인정보 보호법 제28조제1항) ※ 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)
개인정보처리시스템	데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템 (개인정보의 안전성 확보조치 기준 제2조 제1호
위험도 분석	개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절 하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위(개인정보의 안전성 확보조치 기준 제2조 제13호
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 제36조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보보호위원회가 지정한 기관(「개인정보 영향평가에 관한 고시 제2조제3호)
대상시스템	영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템 (「개인 정보 영향평가에 관한 고시」 제2조제4호)

추진근거

- 개인정보 보호법 제33조(개인정보 영향평가)
- 개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상)
- 개인정보 보호법 시행령 제36조(평가기관의 지정 및 지정취소)
- 개인정보 보호법 시행령 제37조(영향평가 시 고려사항)
- 개인정보 보호법 시행령 제38조(영향평가의 평가기준 등)
- 개인정보 영향평가에 관한 고시(개인정보보호위원회고시 제2024-7호) [시행 2024.4.3.]

질의 응답

Q

A

믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다

Privacy by Trust, Trust by Privacy

인용 : 본 교재는 과학기술정보통신부, 개인정보보호위원회, 한국인터넷진흥원에서 제공·공개된 자료가 포함되어 있으며 본 교육과정을 위해 제공됩니다.

※ 저작권 등의 문제로 본 교재의 외부 공개를 금지합니다.