자동처리 되는 개인정보 보호 가이드라인

Privacy by Design 적용사례를 중심으로

2020. 2.

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

자동처리 되는 개인정보 보호 가이드라인

Privacy by Design 적용사례를 중심으로

2020. 2.

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

I

IoT 등에서 자동처리하는 개인정보 보호 10대 수칙

1. 발간배경

IoT 등 센서에 의한 정보 수집, AI기반의 빅데이터 분석 등 새로운 기술은 혁신적인 서비스를 가능하게 하나, 개인정보 처리흐름을 파악하기 어렵고 사후적 대응에는 한계

개인정보 처리 내용에 대한 정보주체의 이해가 더욱 중요

- 정보주체는 빅데이터 분석, AI 등 복잡한 알고리즘과 신기술에 기반한 개인정보 처리에 대한 이해 부족으로 불안감 증대
- 이해부족에 따른 불안감이 서비스나 기업에 대한 불신으로 이어져 분쟁과 소송 등 불필요한 사회적 비용이 발생

사후적 대응보다는 적극적 사전예방이 필요

- 개인정보가 자동으로 처리되는 IoT 환경에서는 열람, 정정·삭제 및 피해 시 배상요구 등 사후적 권리 행사가 어려움
- 특히, 대량의 개인정보가 실시간으로 처리되는 환경에서 침해 발생 시 돌이킬 수 없는 대규모 피해로 이어질 수 있어 적극적 사전예방이 필요

개인정보처리자의 자발적 관행개선 시급

- 법적 책임을 고려하여 실제 개인정보 처리 내용뿐만 아니라 처리하지 않는 내용도 동의를 받는 등의 형식적 동의관행 개선 필요
- 특히, 개인정보를 직접 수집하지 않는 기기 제조업체도 개인정보 보호를 고려하도록 하여 실질적인 개인정보 보호 기반강화 시급

IoT 기기 등으로 개인정보를 자동처리 할 경우 기획단계부터
개인정보 침해 가능성을 충분히 고려하도록 Privacy by Design 개념을 적용하여
개인정보 처리 단계별 고려사항을 사례 중심으로 안내

2. IoT 등에서 자동처리하는 개인정보 보호 10대 수칙

기획

수칙 1

서비스에 꼭 필요한 개인정보인지 확인

- 제공하려는 서비스의 목적과 범위를 명확하게 정의
- 해당 서비스에 꼭 필요한 개인정보 처리(수집·이용, 제공, 파기 등)를 확인하고, 불필요한 개인정보는 수집하지 않도록 기획

수칙 2

개인정보 수집 시 법적 준수사항을 확인

- 정보주체로부터 동의를 받을 의무 등 준수해야 할 개인정보보호 법·제도상의 의무사항을 확인
- 법적 의무를 준수하고 입증할 수 있도록 시스템을 기획

수칙 7

개인정보의 제3자 제공 및 위탁 시 정보주체에게 명확히 안내

- 서비스에 꼭 필요한 개인정보의 제3자 제공은 '목적', '제공받는 자', '제공하는 항목' 등을 명확히 알리고 동의를 받은 후 처리하도록 설계
- 개인정보 처리업무를 위탁하는 경우, 위탁업무의 내용과 위탁받아 처리하는 자를 쉽게 확인할 수 있도록 설계

수칙 8

정보주체가 서비스 해지 시, 개인정보 파기 및 추가 수집 방지

- 법령 상 개인정보 보관의무가 있는 경우 등을 제외하고는 지체 없이 파기되도록 설계
- 자동으로 개인정보를 수집하는 기기가 별도로 운영되는 경우, 추가적인 수집이 발생하지 않도록 기기를 제거·회수하는 절차 마련

수칙 9

사업 종료 시, 정보주체의 권리 보장 방안 마련

- 사업 양도·양수 시, 정보주체에게 개인정보 이전 사실을 통지하고 개인정보 처리정지 요구권 등의 권리를 안내하는 절차 마련
- 서비스를 종료할 경우, 정보주체가 관련 개인정보를 백업할 수 있도록 명확하게 안내하고 해당 기능을 제공할 수 있도록 설계

설계

수칙 3

반드시 필요한 개인정보만 최소한으로 처리

- 꼭 필요한 개인정보만 수집·처리되도록 시스템을 설계하고, 정기적으로 불필요한 개인정보가 수집·처리되지 않도록 확인 절차 마련
- 익명·가명으로도 서비스를 제공할 수 있으면 시스템 설계 시 적용

수칙 4

개인정보 처리단계별 적절한 안전조치 적용

- 최소 인원에게만 접근권한을 부여하고 접속기록 등을 관리
- 암호화조치 등 안전조치가 적용되도록 시스템 설계에 반영

수칙 5

개인정보의 처리절차 및 방법을 투명하게 공개

- 개인정보 처리절차 및 방법 등을 기기 특성에 맞게 공개하는 등 정보주체가 개인정보 처리 내용을 쉽고 명확하게 알 수 있도록 설계

수칙 6

정보주체가 권리 행사를 쉽게 할 수 있도록 보장

- 정보주체가 개인정보의 열람·정정·삭제 등의 요구 방법을 쉽게 확인하고 행사할 수 있도록 시스템 설계

점검

수칙 10

서비스 출시 전, 개인정보 침해 위험요소 점검

- 서비스 출시 전, 본 수칙에 따라 개인정보를 보호하기 위한 조치가 설계에 반영되었는지 확인
- 서비스 개선, 다른 서비스와 연계·연동 등의 변경 시에는 추가적인 개인정보 침해위험이 있는지 점검

Ⅱ

개인정보 보호
10대 수칙별 조치사례

1. 기획

수칙 1 제공하려는 서비스에 꼭 필요한 개인정보인가?

▸ 서비스의 목적과 범위를 명확히 정의하고 해당 서비스에 꼭 필요한 개인정보 처리 절차를 구체화, 불필요한 개인정보는 수집하지 않도록 기획

관련사례 : 서비스 제공에 불필요한 영상정보 수집

[서비스 개요] 음성 명령만으로 음악 재생, 날씨 안내 등의 서비스를 제공하는 AI스피커 서비스 제공

[침 해 위 험] 음성 외에 영상을 수집하는 경우, 음성을 보다 명확히 인식할 가능성은 있으나 사생활 침해 우려는 훨씬 더 커짐

관련조항 : 개인정보보호법 제16조(개인정보의 수집 제한)

[조 치 예 시]
- 음성 인식만으로도 서비스 제공이 가능하므로 불필요한 영상은 수집하지 않도록 카메라는 미설치

수칙 2 개인정보 처리 시 정당한 근거가 있는가?

▸ 개인정보 처리에 적용되는 법적 의무를 확인하고 준수할 수 있도록 시스템에 반영하고 준수 여부를 입증할 수 있도록 기획

관련사례 : 정보주체의 동의 없이 TV시청데이터 수집·이용

[서비스 개요] 사용자의 TV시청데이터를 수집·분석하여 프로그램 추천 및 제안

[침 해 위 험] 스마트TV에 특정 소프트웨어를 설치하여 사용자의 성별, 연령, 소득, TV시청 데이터 등을 수집하여 분석

관련조항 : 개인정보보호법 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법)

[조 치 예 시]
- 수집하려는 개인정보가 동의를 받지 않아도 되는 경우(법령상 의무 수행, 정보주체와의 계약 체결·이행을 위해 불가피한 경우 등)인지를 확인
- 수집·이용하는 개인정보의 항목, 목적, 보유기간, 미동의시 불이익 등을 구체적으로 안내하고 정보주체가 명확하게 인지한 상태에서 동의를 획득했다는 입증방안을 마련

2. 설계

수칙 3 반드시 필요한 개인정보만 최소한으로 처리하고 있는가?

▸ **꼭 필요한 개인정보만 수집 · 처리되도록 시스템을 설계하고 수집정보의 최소화, 수집 장치의 인식 오류 발생 가능성 등을 고려하여 불필요한 개인정보 수집·처리를 정기적으로 확인하는 절차 마련**

관련사례 : AI스피커의 호출어 오인 · 오작동으로 불필요한 개인정보 수집

[서비스 개요] 상시 대기상태에서 호출어 또는 호출센서 등을 통해 활성화된 후, 사용자 목소리를 인식하여 음악재생, 날씨안내 등 해당하는 명령을 수행

[침 해 위 험] 호출명령 인식 오류로 인해 호출명령이 아닌 음성에 기기가 활성화되어, 정보주체가 인식하지 못한 상황에서 대화 내용 등 수집

관련조항 : 개인정보보호법 제16조(개인정보의 수집 제한) 제1항

[조 치 예 시]
- 사용자가 개인정보 수집 여부에 대해 명확히 인식하도록 수집 상태를 표시할 수 있는 기능 마련(예 : 녹음 여부를 알 수 있도록 파란색 LED 점등 등)
- 대기상태 및 호출센서 동작을 On/Off할 수 있는 버튼 등을 설치하여 정보주체가 원하지 않는 시점에서는 음성이 수집되지 않도록 하는 기능 마련

▸ **서비스 제공을 위해 꼭 필요하여 개인정보를 수집하더라도 가능한 익명 · 가명처리하여 활용하는 등 사생활 침해 우려를 최소화하는 방안 마련**

관련사례 : 익명 · 가명처리하지 않아 식별된 개인정보 침해 발생

[서비스 개요] 스마트TV 이용에 따라 생성되는 시청데이터를 분석하여 사용자 맞춤형 콘텐츠 제공

[침 해 위 험] 맞춤형 서비스 제공을 위해 TV시청데이터를 저장 중, 서비스와 무관한 이름, 전화번호 등을 익명·가명처리하지 않고 같이 보관하다가 시청데이터와 함께 유출

관련조항 : 개인정보보호법 제15조(개인정보의 수집·이용)

[조 치 예 시]
- 서비스 제공을 위해 수집하는 개인정보 항목별로 식별성이 필요한지 파악하고, 불필요하면 익명·가명처리하여 활용하도록 시스템을 설계

수칙 4 개인정보가 안전하게 처리되고 있는가?

▸ **개인정보 처리에 대한 접근권한을 꼭 필요한 인원에게만 부여하고 관리자 계정 공유 금지 등의 안전조치를 내부지침에 구체적으로 규정**

관련사례 : 스마트도어벨 업체의 무분별한 접근권한 부여로 인해 개인정보 내부 유출

[서비스 개요] 카메라를 통해 수집한 방문자의 개인영상정보를 분석하여 사용자에게 방문자 정보 제공, 범죄자 구별 등 주택안전을 위한 기능 수행

[침 해 위 험] 개인영상정보 처리 전문업체에 개인정보 처리를 위탁하였고, 수탁업체의 관리 직원이 불필요하게 영상정보를 공유하고 개인적으로 저장하는 등의 내부 유출 사고 발생

관련조항 : 개인정보보호법 제29조(안전조치의무)

[조 치 예 시]
- 저장된 개인영상정보에 대한 접근권한을 최소한으로 부여하고 접속기록 점검 및 관리자 계정 공유금지 등 위탁업체의 개인정보 처리에 대한 철저한 관리·감독 이행

▸ **개인정보가 전송되는 구간(수집장치→서버 등) 등에는 암호화 등 안전조치를 반영하여 시스템을 설계**

관련사례 : 홈 모니터링 기기에서 수집되는 개인영상정보가 쉽게 유출

[서비스 개요] 집 내·외부를 모니터링하는 서비스를 통해 스마트폰, 웹사이트 등으로 언제, 어디서나 모니터링 가능

[침 해 위 험] 홈 모니터링 기기에서 수집한 개인영상정보가 서버로 전송되는 구간에 암호화 조치를 하지 않아 패킷감청 등 간단한 해킹기법으로 개인영상정보가 쉽게 유출

관련조항 : 개인정보보호법 제29조(안전조치의무)

[조 치 예 시]
- 사생활에 밀접한 개인정보를 전송하는 구간에는 설계 시부터 암호화 조치를 적용하여 개인정보가 유·노출되는 피해를 예방할 수 있도록 조치

수칙 5 개인정보 처리절차와 방법을 투명하게 공개하고 있는가?

▸ 개인정보 수집항목, 활용목적, 제3자 제공·위탁 여부 등 처리내역을 정보주체가 이해하기 쉽도록 개인정보 처리방침, 동의서 등에 공개

관련사례 : 정보주체가 명확하게 인지하지 못한 채 개인정보가 제3자 제공

[서비스 개요] 스마트TV 이용 시 수집되는 시청데이터, 음성정보를 광고·마케팅 업체에게 제3자 제공하여 개인 맞춤형 추천서비스 송출

[침 해 위 험] 개인정보 수집·이용 동의서에 제3자 제공에 대한 내용을 작은 글씨로 고지하거나 읽기 어려운 위치로 구성하여 사용자가 인지하지 못하는 문제 발생

관련조항 : 개인정보보호법 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법)

[조 치 예 시]
- 수집, 이용, 저장, 제공, 파기 등 개인정보 처리과정에 대해 개인정보 처리방침, 동의서 등에 인포그래픽, 도식화 등을 활용하여 정보주체가 명확하게 인지하도록 공개
- 정보주체가 명확하게 인지할 수 있는 방안을 제공할 뿐만 아니라 TV화면 내, 스마트폰 앱 등을 통해 언제든지 접근하기 쉬운 위치에 공개하는 것을 기본으로 설정

수칙 6 정보주체가 열람·정정·삭제 등을 쉽게 요구할 수 있는가?

▸ 정보주체가 언제든지 개인정보 이용내역의 열람·정정·삭제 등을 요구할 수 있고 처리자도 신속하게 대응 가능하도록 시스템 설계

관련사례 : AI스피커를 통해 수집된 개인정보에 대해 복잡한 권리 행사 방법 제공

[서비스 개요] 음성정보를 수집하여 음악재생, 날씨안내 등 해당하는 명령을 수행

[침 해 위 험] 정보주체가 인식하지 못한 채 수집 · 저장된 음성정보의 삭제를 요구하고 싶으나 요구방법 안내 미흡 등으로 권리 행사가 어려움

관련조항 : 개인정보보호법 제38조(권리행사의 방법 및 절차)

[조 치 예 시]
- 앱 또는 웹 등 정보주체가 접근하기 쉬운 방법으로 이용내역을 열람할 수 있도록 기능을 제공하여 정정·삭제 등의 권리 행사가 가능하게 하고 자동처리시스템 구축 등 처리자도 신속하게 대응 가능한 방안 마련

수칙 7 개인정보의 제3자 제공 또는 위탁을 명확히 안내하는가?

- 개인정보의 제3자 제공 시, 동의서에 제공되는 개인정보 항목, 목적, 제공받는 자에 대해 명확하게 안내하고 동의를 받도록 규정

스마트TV를 통해 수집한 개인정보를 정보주체의 동의없이 제3자 제공

[서비스 개요] 스마트TV 이용에 따라 생성되는 시청데이터를 분석하여 사용자 맞춤형 콘텐츠 제공

[침 해 위 험] TV시청데이터, 개인 맞춤형 서비스 제공을 위한 분석정보 등을 정보주체에게 동의를 획득하지 않고 제3자 제공하여 원치 않는 광고 문자 수신 등 침해 발생

관련조항 : 개인정보보호법 제17조(개인정보의 제공)

[조 치 예 시]
- 제공 목적, 개인정보 항목, 제공받는 자 등을 동의서에 명확하게 알리고 동의를 받은 후에 제공

- 개인정보 처리업무 위탁 시, 처리되는 개인정보 항목, 처리하는 업무, 수탁업체 등을 개인정보 처리방침 및 동의서에 명확하게 안내

수칙 8 서비스 해지 시, 개인정보를 파기하고 추가수집을 방지하였는가?

- 정보주체가 서비스 해지 시, 법령에 따라 보관의무가 있는 개인정보를 확인
- 보관의무가 없는 개인정보는 즉시 파기될 수 있도록 시스템을 설계하고, 추가 수집 방지 조치(물리적 장치제거, 서버전송금지) 등 명확한 기준을 포함한 내부절차 마련

관련사례 : 집 내부 모니터링 영상 미파기 및 지속적인 수집·이용

[서비스 개요] 집 내·외부를 모니터링하는 서비스에서 SNS 계정으로 로그인하는 서비스를 연동하여 스마트폰으로 언제, 어디서나 모니터링 가능

[침 해 위 험] 홈 모니터링 서비스를 해지한 후에도 연동된 SNS 계정으로 접속되고 해당 기기를 통해 지속적으로 개인정보를 수집

관련조항 : 개인정보보호법 제21조(개인정보의 파기)

[조 치 예 시]
- 정보주체가 서비스 해지 시, 법령상 보존 의무가 없는 개인정보는 지체없이 파기되도록 하고, 자동으로 개인정보를 수집하는 장치는 작동중지, 장치제거 등 추가적으로 수집되지 않도록 설계

수칙 9 서비스 종료 시, 안내를 통해 서비스 선택권 등을 보장하는가?

- 사업 양도 시, 정보주체에게 양수자, 이전되는 개인정보 항목 등을 안내하여 선택권을 행사할 수 있는 기능 마련
- 서비스 종료 시에는 자신의 정보를 백업할 수 있도록 기능을 마련하고 안내

스마트도어벨 사업자의 인수·합병 후 개인정보 처리 관련 사항 미고지

[서비스 개요] 카메라를 통해 수집한 방문자의 개인영상정보를 분석하여 사용자에게 방문자 정보 제공, 범죄자 구별 등 주택안전을 위한 기능 수행

[침 해 위 험] 기존 서비스를 양도 받아 서비스의 고도화를 추진하고 있으나 정보주체는 양도자나 양수자로부터 해당 사실을 안내받지 못함

관련조항 : 개인정보보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)

[조 치 예 시]
- 양도자는 개인정보를 이전하려는 사실, 이전받는 자의 성명, 주소, 연락처, 이전 거부 시 조치방법 안내 (* 양도자가 미안내 시 양수자가 안내)
- 영업 종료 시에는 정보주체가 자신의 개인정보를 백업하도록 안내

3. 점검

수칙 10 기획 · 설계에 따라 개인정보를 처리하는데 위험요소는 없는가?

- 서비스 출시 전, 본 수칙이 적용된 기획 · 설계에 따라 개인정보를 처리하는데 위험요소는 없는지 확인
- 서비스를 개선하거나 타 서비스와의 연계·연동 등 시스템에 변경이 있는 경우, 변경사항에 대한 추가적인 위험요소를 점검하고 조치

홈 모니터링 서비스에서 SNS 계정 연동 시, 위험요소 미파악

[서비스 개요] 집 내·외부를 모니터링하는 서비스에서 SNS 계정으로 로그인하는 서비스를 연동하여 스마트폰으로 언제, 어디서나 모니터링 가능

[침 해 위 험] 사용하던 스마트 홈 모니터링 서비스를 해지하고 타인에게 해당 기기를 판매하였지만, 연동된 SNS 계정은 해제되지 않아 현재 기기사용자의 집 내부영상이 이전 사용자에게 노출

[조 치 예 시]
- 기존 서비스와 SNS 계정 로그인 등 다른 서비스와 연동서비스를 제공하기 전에 개인정보 처리에 따른 추가적인 위험요소가 있는지 점검
- 개인정보 처리과정에서 위험요소가 있는 경우, 본 수칙이 잘 적용되었는지 확인하여 연동서비스 제공에 따른 침해 가능성을 최소화

Ⅲ

참고자료

Privacy by Design의 개념 및 해외 정책사례

1. Privacy by Design의 개념

Privacy by Design은 '프라이버시를 고려한 설계'로 프라이버시 관련 침해가 발생한 이후에 조치를 취하는 것이 아닌 프라이버시 위협을 예측·예상하거나 가능성을 대비하여 서비스 기획·설계 단계 등 사전에 예방하는 개념

※ Privacy by Design은 기존에 건축분야에서 사용되었지만 그 개념이 파생되어 1990년대 중반 캐나다 온타리오주의 정보프라이버시 위원회(IPC : Information & Privacy Commissioner)의 Ann Cavoukian 박사가 언급하면서 알려지기 시작

Privacy by Design 7대 기본원칙(IPC, Ann Cavoukian)

구분	원 칙	내 용
①	사후조치가 아닌 사전예방 (Proactive not Reactive – Preventative not remedial)	프라이버시 침해 사고가 발생한 뒤 조치하는 것이 아닌 침해사건을 예상하고 사전에 예방하는 것
②	초기설정부터 프라이버시 보호조치 (Lead with Privacy as the Default setting)	IT시스템 또는 사업 진행과정에서 개인정보가 보호될 수 있도록 기본으로 설정하여 자동으로 프라이버시가 최대한 보장되도록 하는 것
③	프라이버시 보호를 내재한 설계 (Embedded Privacy into Design)	프라이버시 보호를 설계에 내재화함으로써 프라이버시를 IT시스템 또는 개인정보 처리와 통합·적용하도록 하는 것
④	프라이버시보호와 사업기능의 균형 - 제로섬이 아닌 포지티브섬 - (Retain Full Functionality (positive-sum, not zero-sum))	서비스 제공을 위한 기능성, 편리성 등과 프라이버시 보호 중 어느 하나도 포기하지 않고 프라이버시의 안전한 보호와 사업의 기능성 두 가지 모두 확보하기 위해 노력하는 것
⑤	개인정보 생애주기 전체에 대한 보호 (Ensure End-to-End Security)	개인정보의 수집·이용·저장·제공·파기 전단계에 걸쳐 보호될 수 있도록 안전조치를 적용하는 것
⑥	개인정보 처리과정에 대한 가시성 및 투명성 유지 (Maintain Visibility and Transparency – keep it open)	개인정보 처리과정에 대해 정보주체가 완전하고 명확하게 이해하도록 하여 신뢰성을 제고시키는 것
⑦	이용자 프라이버시 존중 (Respect for User Privacy – keep it user centric)	프로그램, 프로세스 등에서 명시적인 보호체계가 없더라도 사용자의 프라이버시를 보장하기 위한 활동을 수행하는 것

2. Privacy by Design 관련 해외 정책사례

EU – GDPR

▸ 제25조 Data Protection by Design and by Default

IoT, 빅데이터, AI 등 신기술로 인한 개인정보 보호 위협에 대응하기 위해 가장 적합한 프라이버시 보호 방안으로써 'Privacy by Design' 적용을 규정

< 참고 : GDPR 제25조 주요 내용 >

구분		주요내용	비고
1	①	최신 기술과 비용, 개인정보 처리의 성격과 범위, 상황, 목적 등을 포함하여 처리로 인해 개인의 권리와 자유에 대해 발생 가능한 위험성을 고려	권리와 자유 침해 방지
	②	컨트롤러는 처리 수단을 결정한 시점 및 처리 당시 시점에서 데이터 처리 최소화 등 개인정보보호 원칙을 효과적인 방식으로 이행하고 GDPR의 요건을 충족하여야 함	처리 최소화
	③	정보주체의 권리를 보호하기 위한 적절한 기술 및 관리조치(처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등)를 이행하여야 함	정보주체 권리보호 및 안전조치
2	①	컨트롤러는 기본설정(by Default)을 통해, 개별적인 특정 목적에 따라 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리 조치를 이행하여야 함	기본설정에 의한 개인정보 보호
	②	Data Protection by Default는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기간 및 접근가능기간을 설정하는 시점에 적용하여야 함	적용부분 및 시점
	③	개인정보가 정보주체의 개입없이 불특정 다수에게 열람되지 않도록 기본설정(by Default)을 통해 보장	접근제한

EU – ENISA

▸ Privacy and Data Protection by Design

개인정보보호를 위한 다양한 접근방법, 전략, 기술적 요소 등을 검토하는 것을 목적으로 Privacy by Design을 적용하기 위한 사업자를 위해 8가지 핵심전략을 제시

< Privacy by Design 적용을 위한 8가지 핵심전략 >

구분	원 칙	내 용
①	최소화 (Minimise)	프라이버시 침해 가능성을 최소화하기 위해 개인정보의 명확한 활용 목적에 따라 처리되는 개인정보의 양을 최소화하여야 함
②	숨기기 (Hide)	개인정보가 처리되는 과정에서 평문전송 등으로 인해 외부에서 해당 내용을 볼 수 없도록 조치하여야 함
③	분리 (Separate)	개인에 대한 다양한 정보들을 가능한 한 분리해서 저장하여 하나의 DB에서 한사람이 식별되지 못하도록 하여야 함
④	총계화 (Aggregate)	많은 양의 개인정보를 처리할 경우, 가능한 한 개인이 식별되지 않도록 식별자를 최소화하고, 처리 결과는 범주화 등을 통해 식별 불가능하도록 하여야 함
⑤	정보제공 (Inform)	어떤 정보가 어떤 목적으로 어떻게 사용되는지 등 개인정보 처리과정 전반에 대해 정보주체가 투명하게 알 수 있도록 제공하여야 함
⑥	통제 (Control)	'⑤정보제공(Inform)' 전략 적용을 기반으로 정보주체가 개인정보 처리 과정 전반에 대해 명확하게 이해하여 자신의 개인정보의 잘못된 활용이나 보안수준에 대해 권리 행사가 가능하여야 함
⑦	집행 (Enforce)	내부 개인정보보호 정책은 법·제도 의무사항을 모두 반영하여야 하며, 강제적으로 시행되어야 함
⑧	입증 (Demonstrate)	컨트롤러는 개인정보보호 정책이 효과적으로 운영되고 있고, 데이터 유출사고에 즉시 대응이 가능하다는 등 법적 의무사항을 준수하고 있다는 입증할 수 있어야 함

▸ Privacy and Data Protection by Design – from policy to engineering

프라이버시와 정보보호를 위해 다양한 주체(정책입안자, 연구단체, 소프트웨어 개발업체 등)가 수행해야할 활동 및 역할을 권고사항으로 제시

구분	권고사항	비고
정책입안자	개인정보보호 서비스를 촉진하기 위한 새로운 인센티브 매커니즘 개발을 지원하고 촉진	보호활동 촉진
연구단체	다양한 접근법을 통해 개인정보 보호를 위한 엔지니어링 방법을 조사하고 연구 결과는 정책 입안자와 미디어를 통해 공개	보호방안 공개
소프트웨어 개발업체	프라이버시의 속성을 직관적으로 구현할 수 있는 기술을 제시하고, 특히 공개적으로 공동 설립한 인프라 프로젝트에는 개인정보 보호를 지원하는 기술이 반드시 포함되어야 함	보호 기술지원

▸ e-Privacy Directive(전자통신 및 무선장비에 대한 개인정보보호 지침)

전자통신 네트워크와 서비스 제공 시에, 사용자, 가입자의 개인정보와 프라이버시를 보호하기 위해 Privacy by Design 개념과 적합한 다양한 방법을 기술

< Privacy by Design 관련 e-Privacy 지침의 주요 내용 >

구분	내용	비고
전문30	‘전자통신 네트워크와 서비스 제공을 위한 시스템은 최소한의 개인정보만으로 필요한 개인정보의 양을 제한하도록 설계되어야 함’ 이라고 언급하면서 간접적으로 Privacy by Design을 채택	최소 처리
전문46	‘공개적으로 이용 가능한 전자통신 서비스의 사용자 개인정보 및 개인정보보호는 서비스를 제공하는데 필요한 구성요소의 구성에서부터 독립적이어야 함’ 이라고 명시하면서 포괄적인 개인정보보호의 필요성 기술	독립적 구성

미국 - FTC

▸ Protecting Consumer Privacy in an Era of Rapid Change : Recommendations for Business and Policymakers

프라이버시 보호를 위해 Privacy by Design, 단순화된 소비자의 선택, 투명성의 확보 등 실체적, 절차적 원칙을 제시하며 사업자의 조직, 제품 및 서비스 개발 전단계에서 소비자 프라이버시가 지켜져야 함을 강조

< 실체적, 절차적 원칙 주요내용 >

구분	원칙	내용	비고
①	실체적 원칙	데이터 보안, 합리적인 수집제한, 건전한 보존·처리업무 및 데이터의 정확성과 같은 실체적인 프라이버시 보호를 그 사업의 내용에 포함시켜야 함	실질적인 조치 수행
②	절차적 원칙	제품 및 서비스의 라이프 사이클을 통해 포괄적인 데이터 관리절차를 정비하여야 함	전체과정 보호

일본 - GSMA

▸ 모바일 프라이버시 원칙(Mobile Privacy Principle)

기본원칙 중 하나로 'Privacy by Design'을 채택하여 관련 사업자가 새로운 앱 및 서비스, 소프트웨어 및 단말기를 개발할 때 이용자의 개인정보와 프라이버시가 보호될 수 있도록 설계되어야 함을 강조

< 모바일 프라이버시 원칙 >

구분	원칙	내용	비고
①	Framework for mobile privacy - 'Privacy Outcomes'	명확한 프라이버시 보호 프레임을 개발하여 모바일 앱 사용자들의 프라이버시 보호가 내재된 결과물 도출 가능	프라이버시 보호 내재화
②	Codes and standards - 'Privacy by Design'	위치정보, 투명성, 고지 등 개인정보 보호 이슈에 대한 적절한 보호방안뿐만 아니라 PbD를 적용하는 과정에서 모바일 서비스와 이해관계자 간의 프라이버시 관리가 가능	이해관계자간 프라이버시 관리

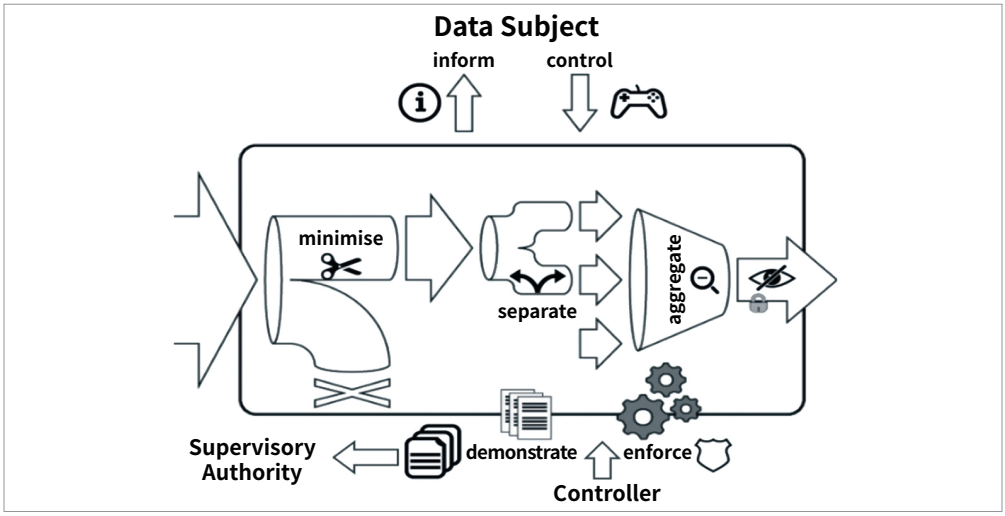
스페인 - AEPD

▸ A Guide to Privacy by Design

모든 처리유형의 도입 단계부터 프라이버시 및 개인정보 보호 원칙을 고려할 필요성을 인지하고 GDPR에서 요구하는 정보처리 원칙(6가지)이 보장될 수 있는 개인정보 보호 목표를 제시하고 이행할 수 있는 개인정보보호 전략을 상세히 설명

< 개인정보보호 목표에 따른 개인정보보호 설계 전략 및 구성도 >

<table>
<tr><th rowspan="2">개인정보보호 목표</th><th colspan="3">개인정보보호 전략</th></tr>
<tr><th colspan="2">데이터 중심</th><th>처리 중심</th></tr>
<tr><td rowspan="2">불연계성
(Unlinkability)</td><td>최소화
(Minimise)</td><td>추상화
(Abstract)</td><td rowspan="2"></td></tr>
<tr><td>분리(Separate)</td><td>숨기기(Hide)</td></tr>
<tr><td rowspan="2">통제
(Control)</td><td colspan="2" rowspan="2"></td><td>통제(Control)</td><td>집행(Enforce)</td></tr>
<tr><td colspan="2">입증(Demonstrate)</td></tr>
<tr><td>투명성
(Transparency)</td><td colspan="2"></td><td colspan="2">정보제공(Inform)</td></tr>
</table>



자동처리 되는
개인정보 보호 가이드라인

Privacy by Design 적용사례를 중심으로

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY