우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 1차 가이드라인

행정안전부
KISA 한국인터넷진흥원

우리 기업을 위한
유럽 일반 개인정보보호법
(GDPR) 1차 가이드라인

서문

한국인터넷진흥원은 행정안전부와 함께 “우리 기업을 위한 유럽 일반 개인정보보호법 (GDPR) 1차 가이드라인”을 발간하게 되었습니다. 이번 가이드라인은 지난 5월 발간한 “우리 기업을 위한 유럽 일반 개인정보보호법 (GDPR) 안내서”를 보다 구체화한 것입니다.

이번 1차 가이드라인에는 유럽연합의 개인정보보호 전문 연구 그룹인 제29조 작업반에서 아래와 같이 발표한 가이드의 주요 내용이 포함되어 있습니다.

- 개인정보 이동권 (The right to data portability)
- DPO 임명 (Data Protection Officer)
- 선임 감독기구 (The lead supervisory authority)
- 고위험 초래 개인정보처리 (Processing likely in a high risk)
- 개인정보영향평가 (Data Protection Impact Assessment)
- 자동화된 의사결정 및 프로파일링 관련 권리(Automated decision-making and profiling)

아울러 제29조 작업반 가이드 외에 우리기업의 현실적으로 필요로 하는 GDPR 준수를 위한 인식제고 및 준비를 위한 절차, 국내 개인정보보호법에는 없는 주요 사안에 대해서 아래와 같이 가이드를 추가였으며 이는 향후 제29조 작업반의 추가 가이드가 발간 및 확정 되면 그에 따라 내용이 일부 수정·보완 될 수 있습니다.

- Data Protection by Design and Default
- 개인정보 국외이전 (Data transfers to third countries)
- 삭제권(잊힐 권리) (Right to erase/‘right be forgotten’)

앞으로 제29조 작업반에서는 개인정보 침해 통지 (Data breach notification), 인증 (certification), 동의(consent), 투명성(transparency), 유럽 개인정보보호 이사회 (EDPS) 구조 등에 대한 가이드를 발간 및 확정할 예정입니다.

향후 우리원은 제29조 작업반의 가이드가 모두 확정되면, 이 내용 등을 종합하여 ‘우리 기업을 위한 GDPR 최종 가이드라인’을 발간할 예정입니다.

미흡하지만 이번 1차 가이드라인이 우리 기업의 GDPR에 대한 이해를 돕는데 조금이나마 도움이 되기를 바라며, 수정이 필요한 사항은 gdpr@kisa.or.kr로 알려주시면 적극 반영토록 하겠습니다.

목차

Ⅰ. 가이드라인 개요

1. 발간 배경

1.1 발간 필요성

▪ 2018년 5월 25일 시행예정인 유럽 일반 개인정보보호법(이하 GDPR)에 대한 개괄적인 안내를 위해 행정안전부와 한국인터넷진흥원(KISA)은 지난 4월 우리 기업을 위한 GDPR 안내서를 발간한 바 있습니다.

▪ 한편, EU 제29조 작업반에서는 지난 '16년 말부터 GDPR 본문에서 규정하는 중요사항 중 기존 EU 개인정보지침(Directive)에 규율하지 않았던 정보주체의 권리 강화, 유럽의 디지털 단일 시장화 등에 대한 사항과 4차 산업 혁명과 기술혁신에 따른 새로운 개념에 대한 세부 적용 사항에 대해서 기업 및 이해관계자들이 쉽게 이해 할 수 있도록 하는 세부 가이드라인을 지속적으로 발간하여 '18년 4월까지 완료할 계획에 있습니다.

▪ 그러나, GDPR에 대한 우리기업의 선제적 대응 및 내부 대응체계 확립 등을 위해서는 EU의 가이드라인 발간이 완료된 시점('18년 4월)에 앞서 GDPR의 주요사항에 대한 1차 가이드라인을 제시할 필요성이 대두되었습니다.

1.2 발간 목적 및 향후계획

▪ 이에 행정안전부와 KISA는 '17년 11월 현재까지 발간된 EU가이드라인(개인정보 이동권, DPO, 선임감독기구, 고위험 초래 개인정보 처리, 개인정보영향평가)을 포함하여 우리기업이 반드시 사전에 숙지해야할 사항이나 기존 국내법에 규율하지 않았던 정보주체의 권리보장 등 중요 사항을 중심으로 제1차 GDPR 가이드라인을 발간하게 되었습니다.

※ EU가이드라인은 최대한 원문내용을 위주로 반영하였으며, EU가이드라인 외에 자체적으로 발간한 가이드라인의 경우 지난 4월 안내서를 발간한 집필진이 참여하여 법해석에 관한 연속성을 유지할 수 있도록 하였습니다.

▪ 본 가이드라인은 GDPR의 본격적인 시행에 대비하여 GDPR이 규정하는 법률에 대한 세부 지침, 구체적 해석 및 이행지침, 대응 방안 등을 우리 기업들이 쉽게 이해하고 대비할 수 있도록 작성되었습니다.

▪ 다만, EU(제29조 작업반)에서 현재까지 발간된 가이드라인 외에 '18년 5월 이전 추가적인 EU가이드라인이 지속적으로 발표될 예정임에 따라 우리 기업을 위한 가이드라인 최종 본은 해당 내용과, 그간의 의견수렴 등을 포함하여 '18년 상반기에 발간될 예정임을 알려드립니다.

현재까지 발간된 가이드라인 현황 및 추후 발간 계획은 다음과 같습니다.

번호	가이드라인 제목	발간 현황
1	· 개인정보 이동권 (The right to data portability)	2016년 발간
2	· DPO 임명 (Data Protection Officer)	
3	· 선임 감독기구 (The lead supervisory authority)	
4	· 고위험 초래 개인정보처리 (Processing likely in a high risk)	2017년 발간
5	· 개인정보영향평가 (Data Protection Impact Assessment)	
6	· 과징금 부과 (The application and setting of administrative fines)	
7	· 개인정보 침해 통지 (Data breach notification)	2017년 초안 발간 (추후 확정 예정)
8	· 자동화된 의사결정 및 프로파일링 (Automated decision-making and profiling)	
9	· 인증 (Certification)	2018년 5월 이전 발간 예정
10	· 개인정보 국외이전 (Data transfers to third countries)	
11	· 투명성 (Transparency)	
12	· 동의 (Consent)	
13	· 유럽 개인정보보호 이사회 구조 (European data protection board)	

2. 가이드라인 구성

2.1 가이드라인 구성 및 주요내용

▪ 본 가이드라인은 총 4장으로 구성되었으며, 주요 내용은 다음과 같습니다.

구분	제목	주요 내용
제1장	안내서 개요	발간 배경 및 GDPR 시행에 따른 주요 변화 등
제2장	GDPR 인식 제고 및 준비	GDPR 준수를 위한 인식 제고
		GDPR 적용 범위
		GDPR 준수 검토 및 모니터링
제3장	기업 책임성 강화	Data Protection by Design and Default
		개인정보 영향평가(DPIA)
		DPO 임명
		개인정보 국외이전
		선임 감독기구 파악
제4장	정보주체 권리 강화	삭제권(잊힐 권리)
		개인정보 이동권
		자동화된 결정 및 프로파일링 관련 권리

2.2 용어의 정의 및 표기

▪ GDPR에서 사용하는 용어가 우리나라 개인정보 보호 관련 법령의 용어와 동일한 의미가 아니거나, 우리말로 번역하여 의미의 혼동을 일으킬 수 있는 경우에는 원문을 그대로 표기 (예 : 컨트롤러, 프로세서, DPO, Data Protection by Design and Default 등) 하였습니다.

※ DPO는 EU GDPR 제37조 'DPO'와 국내 개인정보보호법 제31조 '개인정보보호책임자'는 지정요건, 책무, 자격, 업무독립성, 고용형태 등이 상이한 직위이므로 영어 약어를 그대로 표기함

※ Data Protection by Design and Default를 한국어로 굳이 번역하자면 '개인정보보호 중심 설계 및 설정' 이나 '프라이버시 바이 디자인' 등과 혼용하여 사용되므로 번역을 해서 생길 수 있는 혼동을 방지코자 기존 안내서와 같이 영어 원문을 그대로 표기함

▪ 또한, 중요한 용어이거나 국·영문 병기 시 의미의 전달이 더 정확하고 효율적인 경우 국·영문 병기를 원칙(예:safeguard(보호조치))으로 하고 있으며 자료의 출처는 원문 제목 그대로 표기하여 찾아보기 쉽게 하였습니다.

▪ 아울러, 지난 4월 발행한 「우리 기업을 위한 GDPR 안내서」의 용어의 정의를 이번 가이드라인에서도 동일하게 적용하였습니다.

2.3 가이드라인 활용 및 저작권 표시

▪ 본 가이드라인의 저작권은 행정안전부와 한국인터넷진흥원에 있습니다.

▪ 본 가이드라인은 행정안전부 개인정보보호 종합포털(www.privacy.go.kr)과 한국인터넷진흥원(www.kisa.or.kr) 홈페이지에 게시되어 있습니다.

▪ 본 가이드라인의 내용 중 오류가 있거나 의견이 있을 경우에는 gdpr@kisa.or.kr로 문의하여 주시기 바랍니다.

3. GDPR 시행에 따른 주요변화

1	**넓은 영토적 적용 범위** EU 내에 설립된 기관의 개인정보 처리 활동 외에 1) EU 밖에서 EU에 있는 정보주체에게 재화나 용역을 제공하거나, 2) EU내에 있는 정보주체가 수행하는 활동을 감시(monitoring)하는 기관에 적용됩니다. ※ 위의 경우 제27조에 의거, EU 회원국에 대리인을 지정하여야 합니다.
2	**강력한 제재** '사업체 그룹' 매출 기반으로 과징금(Fines imposed by reference to the revenues of an undertaking)을 부과하며 1) GDPR 규정의 심각한 위반의 경우 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 가운데 더 큰 금액, 2) GDPR 규정의 일반적 위반의 경우 직전 회계연도의 전 세계 매출액 2% 또는 1천만 유로 가운데 더 큰 금액으로 정합니다. ※ 사업체 그룹은 동일한 사업(same undertaking)을 수행하는 것으로 봅니다.
3	**확대된 개인정보의 정의** IP 주소, 쿠키, RFID 등을 개인정보인 '온라인 식별자'의 예시로 들고 있습니다(전문 제30조). 위치정보는 개인정보의 한 유형으로 소개됩니다. 또한, 민감한 성격의 개인정보를 "특별한 유형(special categories)"의 개인정보라고 정의하면서, 유전정보(generic data)와 바이오 정보(biometric data)를 포함했습니다. 개인정보의 가명처리(pseudonymisation) 개념을 도입하였고, 이를 적용하는 경우 Data Protection by Design and Default 의 이행 등 다양한 실익을 거둘 수 있게 하였습니다. ※ 가명화 = 추가정보 없이는 정보주체 식별 곤란 & 추가정보는 기술적·조직적 조치
4	**프로세서에게도 다수의 규정이 직접 적용** Data Protection Directive 95/46/EC 와는 달리 프로세서를 직접 규제하는 내용을 다수 포함하고 있습니다. 프로세서는 적절한 문서화 의무(제30조), 적절한 보안 기준 적용(제32조), 정기 개인정보영향평가 수행(제32조), 개인정보 국외전송 기준 준수(제5장), 국가 감독기구 협조의무(제31조) 등의 의무를 부담합니다. 또한, 프로세서는 제재의 직접적 적용대상이 되며(제83조), GDPR 요구사항을 충족하지 못할 경우 정보주체로부터 배상을 요구 받을 수 있습니다(제79조).
5	**개인정보 처리 원칙의 확립** 개인정보를 처리하는 경우 1) (처리) 적법성, 공정성, 투명성 원칙, 2) (수집) 목적 제한의 원칙, 3) 개인정보 최소화 원칙, 4) 정확성 원칙, 5) 저장 제한 원칙, 6) 무결성 및 기밀성 원칙 (이상 제5조) 등 6가지 원칙을 모두 준수하여야 합니다. 컨트롤러는 이와 같은 원칙을 준수함을 증명(demonstrate compliance) 해야 하는 의무(소위 "책임성 원칙(accountability principle)")를 부담합니다.

6	**적법 처리 기준의 상향**
	개인정보의 (처리) 적법성, 공정성, 투명성 원칙에 따라 개인정보의 처리는 법률에서 허용한 어느 하나 이상의 요건에 해당해야 적법 처리로 인정됩니다.
7	**개인정보 국외이전 메커니즘 확립**
	국외이전 = 적정성 평가(Adequacy Decision) 또는 ["적절한 보호조치(appropriate safeguards)" 제공 + 정보주체 권리 행사 가능 + 효과적인 법적 구제수단 존재]의 경우에만 가능합니다. 적절한 보호조치에는 구속력 있는 기업 규칙(Binding Corporate Rules), 표준계약서(Standard Contractual Clauses) 등이 있습니다. 기타, 1) 승인된 행동강령, 2) 인증 제도가 새롭게 추가되었습니다. Derogations(명시적 동의, 계약 이행 등)에 의한 국외이전도 가능합니다.
8	**개인정보 유출통지 제도의 도입**
	컨트롤러는 개인정보 유출 사실을 알게 된 때로부터 가능한 경우 72시간 내에 감독 당국에 신고해야 하며, 정보주체의 자유와 권리에 고 위험(high risk)이 예상될 때에는 부당한 지체 없이(without undue delay) 유출 사실을 정보주체에게 통지해야 합니다. 프로세서는 개인정보 유출 사실을 알게 된 때엔 컨트롤러에게 그 사실을 부당한 지체 없이 알려야합니다.
9	**정보주체의 권리 확대**
	컨트롤러의 투명성 의무 부담에 더하여, 정보주체는 열람권(제15조), 정정권(제16조), 삭제권(제17조), 처리제한권(제18조), 개인정보 이동권(제20조), 반대권(제21조), 프로파일링을 포함한 자동화된 처리의 결과를 적용받지 않을 권리(제22조) 등의 권리를 갖습니다.
10	**DPO의 의무 지정**
	공공기관(public authorities)이거나, 컨트롤러나 프로세서의 핵심 활동이 1) 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링에 해당하거나, 2) 민감정보나 범죄경력 및 범죄 행위에 대한 대규모 처리인 경우 DPO를 의무적으로 지정해야합니다.
11	**책임성과 거버넌스 강화**
	1) 처리 활동의 세부 기록 유지(제30조), 2) 고 위험 처리에 대한 개인정보영향평가 수행(제35조), 3) DPO 지정(제37조), 4) 개인정보 유출통지 및 종합적 기록 유지(제33~34조), 5) Data Protection by Design and Default이행(제25조) 등 개인정보 처리에 대한 책임성 및 거버넌스를 강화했습니다.
12	**One Stop Shop의 도입**
	컨트롤러, 프로세서는 주 사업장 또는 단일 사업장에 대한 선임 감독기구에 의해 규율됩니다.(제56조). 그러나 선임 감독기구는 다른 연관된 기관과 협력해야 하며, 다른 기관이 특정 사안에 관여할 수도 있습니다.

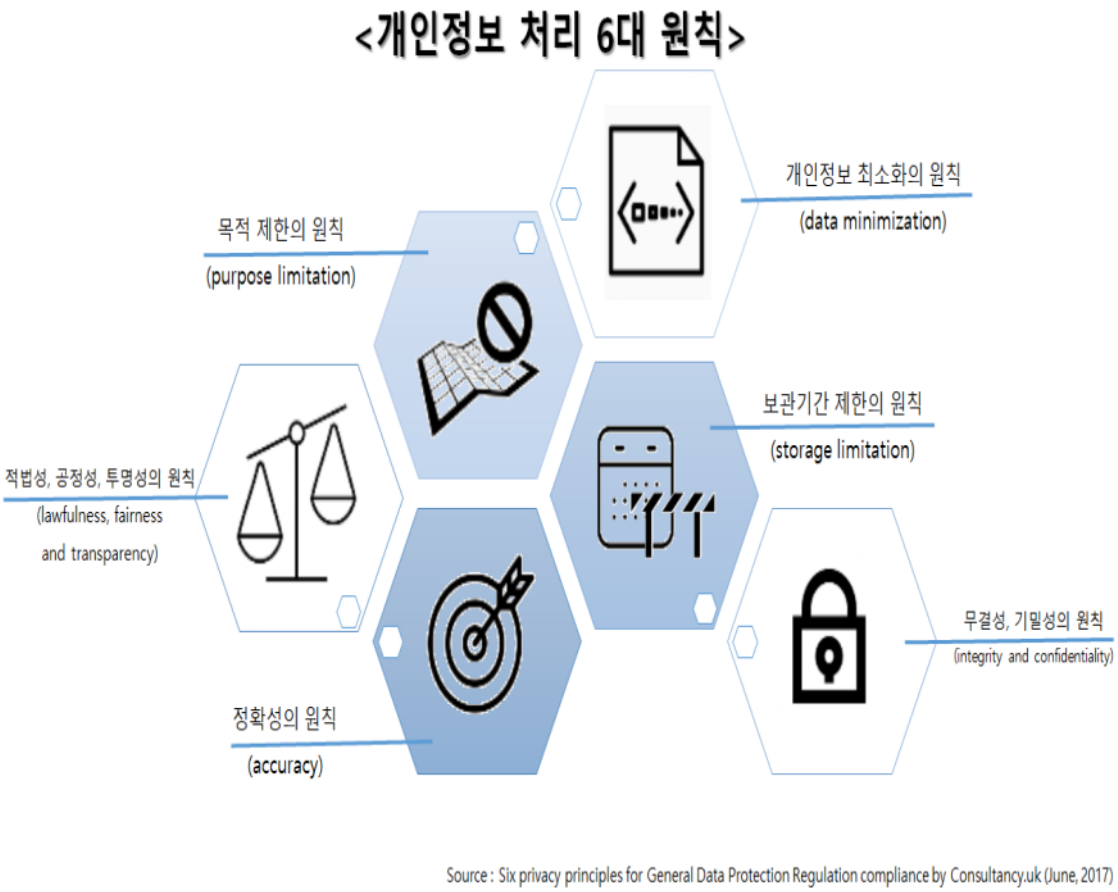
Ⅱ. GDPR 인식 제고 및 준비

1. GDPR 준수를 위한 인식제고 (Awareness)

Check List

- 조직의 의사결정을 내릴 수 있는 관리자 그룹의 GDPR-Readiness Program 참여에 대한 약속을 확보합니다.
- GDPR의 주요 내용을 확인하고, 조직 전체에 이를 알리는 활동을 수행합니다.
- 현재의 개인정보 처리와 GDPR이 요구하는 개인정보 처리의 차이를 분석합니다.
- DPO를 선임합니다.
- 개인정보처리시스템을 개선하고, 정보주체와의 접점에서의 커뮤니케이션 방식을 변경합니다. 정보주체 권리 보장, 개인정보 침해 신고 및 통지, 개인정보 영향평가 수행, 프로세서 관리방안 마련 등을 이행합니다.
- 책임성 원칙에 따른 입증 책임을 증명할 수 있는 방안을 마련하여 이행합니다.

GDPR 준수는 GDPR에 대한 인식활동에서 시작하며, 개인정보 처리의 6대 원칙 및 이의 입증을 의미하는 책임성 원칙(Accountability)의 증명으로 마무리 되는 과정입니다.



Source : Six privacy principles for General Data Protection Regulation compliance by Consultancy.uk (June, 2017)

< GDPR 준수를 위한 인식제고 (Awareness) >

1. 관리자 그룹의 참여에 대한 약속 확보
2. 조직 전체에 알리는 활동 수행
3. 현재와 GDPR이 요구하는 차이를 분석
4. DPO 선임
5. 액션 플랜 이행 (정보주체 권리 보장, 영향평가 등)
6.책임성 원칙에 따른 입증 책임을 증명 할 방안 마련

1.1 조직의 의사결정에 관여하는 관리자들의 참여를 확보하십시오.

- 조직의 의사결정을 내릴 수 있는 상위 관리자 그룹(Senior Management)이 GDPR 대응 프로그램에 적극 참여하겠다는 약속을 확보하는 것으로 GDPR 준수를 위한 인식 활동이 시작됩니다.

- 이에 참여하는 부서는 법무나 정보보호 관련 부서뿐만 아니라, 고객관리, 인사, 재무, 마케팅, 시스템 개발 등 다양하게 구성되어야 합니다.

- 이후, GDPR 준수활동에 참여하는 다양한 부서는 조직의 위험 등록부(Risk Register)에 GDPR 위반에 따른 재정적, 운영적, 평판적 위험을 기록하고, 이를 지속적으로 관리하는 방식으로 GDPR 준수를 위한 인식을 유지할 수 있습니다.

1.2 GDPR의 주요 내용을 확인하고, 이를 조직에 알리는 등 인식제고 활동을 수행 하십시오.

▪ GDPR의 주요 내용

① 넓은 지역적 적용 범위 : 유럽연합 외의 지역에서 개인정보를 처리하는 경우라 하여도, 1) 유럽연합의 정보주체에게 재화나 서비스를 제공하는 경우, 또는 2) 유럽연합의 정보주체가 수행하는 활동을 모니터링 하는 경우 GDPR이 적용될 수 있습니다. 또한, 이런 경우 유럽연합 내에 대리인(representative)을 지정하여야 합니다.

② 강력한 제재 : '사업체 그룹(a group of undertakings)'의 연간 매출을 기반으로 과징금을 부과하며, GDPR의 심각한 위반에 해당하는 경우 2천만 유로 또는 직전 회계연도의 전 세계 매출액의 4% 가운데 더 큰 금액을 과징금으로 부과할 수 있습니다.

③ 프로세서의 책임 강화 : 개인정보보호지침(Data Protection Directive 95/46/EC)과는 달리 프로세서가 개인정보처리와 관련한 책임을 직접 부담하는 경우가 다수 포함되었습니다. 개인정보 처리활동의 기록(제30조), 적절한 보안기준 적용(제32조), 개인정보 영향평가 수행의 지원(제35조), 개인정보 국외이전 메커니즘 준수(제5장), 국가 감독기구 협조(제31조) 등의 내용이 이에 해당합니다.

④ 개인정보 유출 신고 및 통지 제도 도입 : 컨트롤러는 개인정보 유출 사실을 알게 된 때로부터 가능한 경우 72시간 내에 감독 당국에 신고해야 하며, 정보주체의 자유와 권리에 고 위험(high risk)이 예상될 때에는 부당한 지체 없이 유출 사실을 정보주체에게 통지해야 합니다.

⑤ 정보주체의 권리 확대 : 정보주체는 개인정보 열람권(제15조), 정정권(제16조), 삭제권(제17조), 처리제한권(제18조), 이동권(제20조), 반대권(제21조), 프로파일링 등 자동화된 의사결정에 반대할 권리(제22조) 등의 권리를 가집니다.

⑥ 책임성 및 거버넌스의 강화 : 개인정보 처리의 6대 원칙을 이행하는 한편,

이를 객관적으로 입증할 수 있어야 합니다. 특히, 개인정보 처리원칙의 이행을 입증하는 것을 책임성 원칙이라 합니다.

참 고

▪ **GDPR 인식제고 활동**

① 개인정보보호 지식 수준에 대한 조직원 대상의 설문조사
② GDPR 교육 활동의 체계적 조직 및 시행 (E-Learning 및 Webinar 포함)
③ 경영진의 GDPR 준수 의지의 공식적 선언
④ 조직 웹사이트에 GDPR 채널 개설
⑤ GDPR 준수 활동의 진척 공유
⑥ GDPR 컨퍼런스, 세미나 참석 독려
⑦ GDPR 영상, 배너, 포스터, 인포그래픽 제작 및 배포
⑧ 부서별 수행해야 할 주요 체크리스트 작성 및 배포 등

1.3 GDPR이 요구하는 개인정보 처리 방식과의 갭 분석을 하십시오.

▪ GDPR에 도입된 다양한 개인정보 처리 요구사항을 파악해야 합니다. 특히, Data Protection by design and default를 항상 고려해야 합니다.

▪ 개인정보의 암호화를 포함하는 다양한 개인정보보호 기술(PETs, Privacy Enhancing Technologies)의 적용을 고려한 개인정보 처리방식의 차이점을 확인합니다.

▪ 개인정보의 적법한 처리 기준, Privacy Notice의 내용, 이용자 권리보장 방식, 개인정보 침해 신고 및 통지 절차, 개인정보 처리활동의 기록(문서화) 등 다양한 측면에서 갭 분석을 진행합니다.

1.4 DPO를 선임하십시오.

▪ 개인정보보호활동을 이끌어갈 DPO를 선임해야 합니다. DPO는 조직 내에서 지정할 수도 있고, 조직 외부에서 계약을 통해 확보할 수도 있습니다. 동일한 개인정보 처리활동에 관여하는 사업체 그룹의 경우 1인의 DPO를 지정할 수 있습니다.

▪ 개인정보 인식제고 활동에 DPO가 중요한 역할을 할 수 있도록 자원을 적극 지원해야 합니다.

1.5 액션 플랜을 이행 하십시오

▪ 갭 분석을 통해 확인된 미비점을 개선하기 위한 활동을 이행합니다. 정보주체 권리 보장, 개인정보 침해 신고 및 통지, 개인정보 영향평가 수행, 프로세서 관리방안 마련 등이 이에 해당합니다.

▪ 액션 플랜의 이행은 중요한 사항의 누락이 발생하지 않도록 체크리스트 기반으로 점검되어야 합니다. 체크리스트는 감독 기관의 가이드, 법원의 GDPR 조문 해석, 업계 사례 등에 따라 적절히 업데이트 되어야 합니다.

1.6 책임성 원칙을 입증할 수 있도록 적절히 문서화를 수행하십시오.

▪ 개인정보 처리원칙을 준수하였음을 입증할 수 있도록 적절한 문서화를 수행해야 합니다. 이는 개인정보 영향평가(DPIA)의 산출물일 수도 있고, 회의록, 보고서, (자동화된) 로그 기록 등의 형태일 수도 있습니다.

▪ 개인정보 처리활동에 대한 책임성 원칙 준수 기록은 단순히 발생한 사실에 그쳐서는 안 되며, 모든 개인정보 처리 과정에 개인정보 처리 6대 원칙을 고려하여 체계적으로 기록되어야 합니다.

▪ 위 1.1~1.6의 활동은 지속적으로 수행되어야 하며, GDPR 시행 이후에도 정기적으로 반복되어야 합니다. 조직 구성원의 학습 곡선(Learning Curve)을 고려하여, 지속적인 인식제고 활동을 이행하십시오.

꼭 알아두기

- GDPR 준수를 위한 활동은 인식제고 활동으로 시작합니다. 이를 위해, 조직 내 여러 부서가 참여해야 합니다.
- 인식제고를 위해 GDPR의 주요 내용을 조직 내 적절히 알려야 합니다. 설문조사, 교육, 경영진 선언, GDPR 웹페이지 개설, 배너나 포스터의 제작 및 배포 등을 수행할 수 있습니다.
- DPO를 지정하고, 갭 분석으로 확인된 액션 플랜을 이행하는 한편, 책임성 원칙의 준수를 입증하기 위한 문서화에 관심을 기울이십시오.
- GDPR 준수를 위한 인식제고 활동은 지속, 반복적으로 수행되어야 합니다.

관련 조문 및 근거

- 제5조(개인정보 처리에 관한 원칙)
- 전문 제26조

2. GDPR 적용 범위

Check List

■ 물적 적용범위에 해당하는지 확인하십시오.(개인정보의 처리에 적용됩니다.)

① 자동화된 수단에 의한 개인정보의 처리에 GDPR이 적용됩니다.

② 자동화된 수단이 아닌 경우에도 GDPR이 적용되는 경우가 있습니다. 파일링 시스템의 일부를 구성하거나, 파일링 시스템의 구성을 목적으로 하는 개인정보의 처리에 GDPR이 적용됩니다.

■ 지역적 적용범위에 해당하는지 확인하십시오(유럽연합 외의 국가에서도 적용될 수 있습니다.).

① 유럽연합의 데이터 컨트롤러나 프로세서의 사무소나 거점(establishment)이 수행하는 개인정보의 처리 활동에 GDPR이 적용됩니다.

② 유럽연합 밖에서 유럽연합 정보주체에게 재화나 용역을 제공하는 경우, GDPR이 적용됩니다.

③ 유럽연합 정보주체가 유럽연합에서 수행하는 활동을 모니터링 하는 경우, GDPR이 적용됩니다.

■ 인적 적용범위에 해당하는지 확인하십시오(살아있는 자연인의 개인정보를 처리하는 컨트롤러 또는 프로세서에 적용됩니다.).

- 자연인의 개인정보를 처리하는 데이터 컨트롤러 또는 프로세서에 GDPR이 적용됩니다.

■ GDPR 적용 예외에 해당하는지 확인하십시오.

- 일정한 요건에 해당하는 경우, GDPR 적용 예외에 해당할 수 있습니다.

< GDPR 적용 범위>

2.1 물적 적용범위에 해당하는지 확인하십시오.(개인정보의 처리에 적용됩니다.)

- 개인정보가 자동화된 수단에 의해 처리되는 경우 GDPR이 적용됩니다. 단, 자동화된 수단에 의하지 않더라도, 파일링 시스템의 일부를 구성하거나 파일링 시스템의 구성을 목적으로 하는 개인정보의 처리에 GDPR이 적용될 수 있습니다.

- 익명 정보(anonymous data)는 개인정보에 해당하지 않으므로 GDPR이 적용되지 않습니다. 또한, 특정 기준에 따라 구성되지 않은 물리적 파일이나 파일의 집합물(소위 ‘ad-hoc paper records’)에는 적용되지 않습니다.

2.2 지역적 적용범위에 해당하는지 확인하십시오.(유럽연합 외의 국가에서도 적용될 수 있습니다.)

- 유럽연합의 데이터 컨트롤러나 프로세서의 사무소나 거점(establishment)이 수행하는 활동에 GDPR이 적용됩니다.

- 사무소 또는 거점(establishment)이란 개인정보 보호의 관점에서 특정 조직이 어느 유럽연합 회원국의 사법관할권 영향에 놓이게 되는지를 결정하는 개념으로, 1) GDPR에 따른 정보주체의 권리를 어느 국가에서 행사할 수 있는지, 2) 법 집행 활동에 있어 어느 감독 당국이 관여하는지, 3) 어느 국가에서 사법절차가 진행될 수 있는지 등에 영향을 미칩니다. 사무소 또는 거점은 법률적 형태에 구속되지 않는 폭 넓고 유현한 표현이며, 실질적이고 효과적인 활동을 수행하는 조직은 사무소에 해당할 수 있습니다.

- 유럽연합 밖에서 유럽연합 정보주체에게 재화나 용역을 “제공(offering)” 하는 경우 또는 유럽연합 정보주체가 유럽연합에서 수행하는 활동을 모니터링 하는 경우 GDPR이 적용됩니다. 이러한 경우 반드시 유럽연합 내에 대리인을 지정해야 합니다.

- 재화나 용역을 ‘제공’한다고 판단될 수 있는 요소는 다음과 같은 것이 있습니다.

① 언어(소재 또는 거주 국가의 고객과 관련 없는 유럽연합 회원국의 언어를 사용)
② 통화(소재 또는 거주 국가에서 일반적으로 사용하지 않는 유럽연합 회원국의 통화를 사용)
③ 도메인 이름(웹사이트의 도메인 이름이 유럽연합 회원국의 최상위 도메인 명칭을 사용함. 예: .de, .fr 등)
④ 회원국 시민 언급(재화나 서비스를 홍보하기 위해 유럽연합 회원국 시민을 언급함)
⑤ 소비자 기반(유럽연합 내에 높은 비율의 소비자를 보유하고 있음)
⑥ 광고 타게팅(유럽연합 회원국의 정보주체를 목표로 광고를 제공함) 등

▪ 정보주체의 활동을 '모니터링' 한다는 의미는 그의 활동을 감시(surveillance)하는 것이 아니라, 정보주체의 온라인에서의 활동을 지속적으로 추적(tracking)하는 것을 의미합니다. 맞춤형 광고의 제공을 위한 이용자 브라우징 정보를 수집, 축적, 분석하는 행위는 모니터링에 해당합니다.

2.3 인적 적용범위에 해당하는지 확인하십시오.(살아있는 자연인의 개인정보를 처리하는 컨트롤러 또는 프로세서에 적용됩니다.)

▪ 법인의 정보나 사망한 사람의 개인정보를 처리하는 경우 GDPR이 적용되지 않습니다. 단, 유럽연합 회원국이 사망한 사람의 개인정보를 보호하기 위해 개별적으로 별도의 입법을 하는 것은 가능합니다.

▪ GDPR이 적용되는지 여부를 고려할 때, 정보주체인 자연인의 국적이나 거주지가 반드시 유럽연합 회원국일 필요는 없습니다.

2.4 GDPR 적용 예외에 해당하는지 확인하십시오.

▪ 다음의 경우에는 GDPR이 적용되지 않습니다. (제2조 제2항, 전문 제13~20조)

① EU 법률의 적용 범위를 벗어나는 활동
② EU 공통의 해외, 안보정책과 관련된 활동
③ 관할 감독기구가 범죄 및 이와 관련된 사안의 예방, 수사, 탐지, 기소 등의 목적으로 수행하는 활동 (예, Law Enforcement Agencies Directive(EU 2016/618)이 적용되는 활동)

④ 자연인이 수행하는 순수한 개인(purely personal) 또는 가정 활동(household exemptions)

⑤ EU기관, 기구, 사무소 등이 처리하는 개인정보에 대해서는 GDPR이 아닌 별도의 규칙(Regulation 45/2001/EC)이 적용됨.

⑥ 중개서비스제공자의 책임과 관련하여서는 GDPR이 아닌 전자상거래(e-commerce)지침(2000/31/EC)이 적용됨.

꼭 알아두기

- GDPR은 통상 자동화된 수단에 의한 개인정보의 처리에 적용되지만, 비자동화된 수단에 의한 경우에도 적용될 수 있습니다.
- GDPR은 유럽연합 밖에서의 개인정보 처리활동에도 적용될 수 있으며, 이러한 경우 유럽연합 내에 대리인(representative)을 지정해야 합니다.
- GDPR은 살아있는 자연인의 개인정보를 처리하는 경우 적용됩니다. 법인의 정보나 사망한 사람의 개인정보에는 일반적으로 적용되지 않습니다.
- GDPR 적용 예외도 꼭 확인하시기 바랍니다.

관련 조문 및 근거

- 제2조(물적 적용범위)
- 제3조(지역적 적용범위)
- 제27조(유럽연합 내에 설립되지 않은 컨트롤러나 프로세서의 대리인)
- 전문 제13~20조
- 전문 제23~27조

3. GDPR 준수 검토 및 모니터링

Check List

- 보유 대상 개인정보의 유형을 전반적으로 파악하십시오.
  (목록을 문서화해 유지하고, 특히 민감정보와 고위험 개인정보는 위험수준에 대한 세밀한 평가를 수행)
- 다양한 개인정보 처리의 방식을 상세히 규명 하십시오.
  (자동화된 처리와 수기 처리로 이뤄지는 다양한 개인정보 처리 방식을 상세 규명)
- 처리되는 개인정보의 규모를 파악하십시오.
- 개인정보 목록 및 흐름을 파악하여 적절한 모니터링 및 통제가 이루어 질수 있도록 하십시오.
- 자체 GDPR 대응체계를 마련하십시오.
- 조직 특성에 맞는 다양한 보안이슈를 관리 하십시오.

< GDPR 준수 검토 및 모니터링>

3.1 보유 대상 개인정보 유형을 파악하십시오.

▪ GDPR 하에서 컨트롤러와 프로세서는 특정 개인정보를 어디에 보관하고 있는지 정확히 식별할 수 있어야 합니다. GDPR에서 '개인정보'는 식별되었거나 또는 식별 가능한 자연인과 관련된 모든 정보를 의미합니다. 즉, 이름,

주소, 전화번호, 신용카드 번호 뿐만 아니라 심지어 IP주소, 위치정보까지 포함된 개인에 대한 모든 데이터로 봐야 합니다.

▪ 특히, 기기, 응용프로그램, 도구(tool), 프로토콜 등에 의해 제공되는 정보나 쿠키식별자, RF 식별태그 등을 온라인 식별자로서 포괄적으로 포함시키고 있는 점(예: IP, MAC, IMEI, 안드로이드 ID 등)과 위치정보를 하나의 속성으로 이해하기 보다는 식별자로서 의미를 두는 점은 유의할 필요가 있습니다.

▪ GDPR에서 민감정보(Special categories of personal data)는 국내 보다 훨씬 포괄적인 유형을 포함하고 있습니다. 인종·민족, 정치적 견해, 종교·철학적 신념, 노동조합의 가입여부를 드러내는 개인정보, 유전자 정보, 자연인을 고유하게 식별할 수 있는 바이오인식정보, 건강 관련 정보, 성생활·성적 취향에 대한 정보 등 다양한 유형들을 포함합니다.

※ 주요 민감정보 내용

① 유전정보: 자연인의 생리 또는 건강에 관한 고유정보 (염색체, DNA, RNA 등 분석 정보)
② 바이오인식정보: 자연인의 고유한 식별을 허용하거나 확인하는 정보 (얼굴 이미지, 지문정보 등)
③ 건강 관련 정보: 신체적 또는 정신적 건강과 관련된 개인정보 (건강 관리 서비스 제공 포함)

▪ 민감정보의 처리는 일반적으로 금지되나, 정보주체의 명시적 동의(explicit consent)가 있는 경우 등 아래 10가지 예외사항에 한해 처리가 허용됩니다. 민감정보의 활용 측면에서 본다면 오히려 국내 기준이 더 엄격하다고 볼 수도 있습니다.

※ 민감정보 처리 적법요건 (제9조 2항)

① 정보주체가 명시적 동의(explicit consent)를 한 경우
② 고용과 사회 안보 및 사회보장법 또는 단체협약에 따른 의무의 이행을 위해 필요한 경우
③ 정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위하여 필요한 경우

④ 비영리기관이 그 기관의 구성원 또는 과거 구성원 또는 그 목적과 관계되어 정보주체의 동의 없이 그 기관 밖으로 공개되지 않는 조건으로 처리가 수행되는 경우
⑤ 정보주체가 일반에게 공개한 것이 명백한 정보인 경우
⑥ 법적 청구권의 설정, 행사 또는 방어를 위하거나 법원이 재판기관으로 행동할 때
⑦ EU 또는 회원국 법에 근거하여 중대한 공익 실현에 필요한 경우
⑧ 예방의학이나 직업의학의 목적으로, 건강이나 사회복지 시스템과 서비스의 관리를 위하여 필요한 경우
⑨ EU 또는 회원국 법에 근거하여 공중보건 영역에서 공익을 이유로 필요한 경우
⑩ 제89조 제1항에 따른 공익을 위한 기록보존 목적, 과학적 또는 역사적 연구 또는 통계적 목적으로 필요한 경우

▪ 민감정보 중 유전정보, 바이오인식정보, 건강 관련 정보는 회원국별 추가적인 조건(한도 포함) 도입이 가능하므로 회원국별 별도 규정을 살펴볼 필요가 있습니다. 그리고, GDPR은 민감정보 유형에 유죄 판결 및 형사범죄 정보를 포함시키지 않고 있어 국내 기준과 차이가 있음을 이해할 필요가 있습니다.

참 고

[국내 개인정보보호법 제23조 민감정보 정의]
- 1) 사상·신념, 2) 노동조합·정당의 가입·탈퇴, 3) 정치적 견해, 4) 건강, 성생활 등에 관한 정보, 5) 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보를 의미
- 같은 법 시행령 제22조는 유전정보, 범죄경력에 관한 정보도 민감정보에 해당한다고 규정

3.2 다양한 개인정보 처리의 방식을 상세히 규명하십시오.

▪ GDPR에서는 개인정보 처리를 자동화된 수단에 의한 처리(processing)로 한정하지 않고 있습니다. 개인정보를 활용한 대부분의 활동이 처리에 해당하되, 다른 사람이 처리하고 있는 개인정보를 단순히 전달 또는 통과만 시켜주는 행위는 처리에 해당하지 않습니다.

▪ 국내에서는 개인정보 처리 유형을 수집-저장-이용-제공-폐기의 단계로 구분하는 게 일반적인데, 이러한 개인정보 Life-Cycle 관점의 정형화된 처리

단계로 주요 처리 현황을 파악하되 이러한 정형화된 범주에 포함되지 않는 처리 방식에 대해서도 빠짐없이 파악할 수 있도록 해야 합니다.

참 고

[GDPR 제4조 2항]

- 처리는 수집, 기록, 조직, 구조화, 저장, 적응 또는 변경, 검색, 협의, 사용, 전송에 의한 노출, 보급 또는 기타 이용 가능, 정렬 또는 조합, 제한, 삭제 또는 파기를 포함

[국내 개인정보보호법 제2조 제2호]

- 처리란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그밖에 이와 유사한 행위를 말함

3.3 처리되는 개인정보 규모를 파악하십시오.

▪ GDPR에서는 전체적 또는 부분적인 자동화된 수단에 의해 처리된 개인정보(예: 전자적 데이터베이스, 컴퓨터로 운영되는 파일링 시스템 등)는 물론 비자동화된 수단에 의한 수기처리와 같은 개인정보 처리라도 파일링 시스템의 일부를 구성하는 경우 적용 대상으로 보고 있습니다. 따라서 이를 감안해 조직 내 어디에 어느 정도 규모로 개인정보를 보유하고 있는지 파악을 해야 합니다.

※ 파일링 시스템(filing System): 기능적 또는 지리적 근거로 집중, 비집중 또는 분산되는지 여부와 관계없이, 특정한 기준에 따라 접근 가능한 모든 구조화된 개인정보 집합

참 고

[국내 개인정보보호법 제2조 제4호]

- “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

3.4 개인정보 목록 및 흐름을 파악하여 적절한 모니터링 및 통제가 이루어 질수 있도록 하십시오.

▪ 조직 내 개인정보 목록 및 흐름을 분석할 수 있는 프로세스를 정립하여 개인정보 목록을 지속적으로 갱신하고 관련 흐름을 파악해야 합니다. 해당 프로세스에는 아래 사항들이 필수적으로 포함될 필요가 있습니다.

① 개인정보를 이용하는 핵심 비즈니스 프로세스
② 개인정보의 출처
③ 고위험의 개인정보 식별을 포함한 처리되는 개인정보의 범주
④ 수집된 초기 목적 및 후속적 2차 목적을 포함한 개인정보의 사용 목적
⑤ 제3자에 대한 개인정보 공개, 프로세서 및 공급업체로의 전송을 포함한 개인정보의 잠재적 수령인
⑥ (개인정보 흐름 내에서) 조직이 컨트롤러, 프로세서 또는 공동 컨트롤러로 활동하는 경우
⑦ 개인정보의 주요 시스템 및 저장소
⑧ (개인정보 흐름 내에서) 개인정보가 국제적 경계를 넘어 전달되어 다른 법률, 규정, 표준 또는 프레임워크를 따르는 경우
⑨ 개인정보의 저장/파기 요구사항 및 이들 요구사항의 기준

▪ 조직이 처리하는 개인정보 범주 목록을 유지하여 각 개인정보 범주가 사용되는 목적을 문서화하고, 조직 전반의 프로세스에 걸친 개인정보 흐름을 문서화하여 조직이 처리하는 개인정보 범주와 해당 정보 처리와 관련된 위험수준을 조직이 이해할 수 있도록 해야 합니다.

▪ 특히, 조직이 처리한 고위험에 속하는 개인정보에 대해서는 명시적 식별 및 문서화가 반드시 필요합니다. 많은 양의 개인정보가 처리되는 경우 위험수준이 높아지는 것이 당연하므로 다량의 개인정보가 처리되는 유형은 특별한 주의 관리가 필요합니다.

※ 고위험에 속하는 개인정보에 대한 자세한 내용은 제3장의 2. 개인정보 영향평가 부분을 참고하시기 바랍니다.

- GDPR 하에서 컨트롤러와 프로세서는 특정 데이터를 어디에 보관하고 있는지 정확히 식별할 수 있어야 합니다. GDPR에서는 자연인의 개인정보 자기결정권을 강화하는 방향으로 정보주체의 권리를 보장하고 있습니다. 기존 Directive에 담겨있던 정보주체의 열람권·정정권 외에 개인정보 이동권 (Right to data portability), 삭제권(Right to erase/'right be forgotten'), 자동화된 결정 및 프로파일링 관련 권리 (Right to related to automated decision making and profiling) 등의 도입이 대표적입니다.

- 정보주체가 본인 권리를 행사할 경우 컨트롤러는 '부당한 지체 없이', 그리고 '늦어도 1개월 이내'에 관련 정보를 제공할 의무가 있습니다. 즉 정보주체의 요구에 따라 신속히 대처하기 위해 조직에서 처리되고 있는 개인정보 처리 모니터링 체계 및 개인정보를 적절히 탐색·통제할 수 있는 기술적인 방안이 수립되어야 합니다.

- 최근 클라우드 기술의 대중화로 기업 내부에서 관리되지 않는 데이터들이 지속적으로 증가하고 있습니다. 데이터 저장의 효율성을 높일 수 있는 전략이지만 데이터에 대한 조직 자체의 통제력이 떨어지는 만큼 철저한 관리적 조치가 필수적입니다. 사이트와 시스템 간 이동 시에 데이터 유실을 방지하고 정보 탐색이 용이할 수 있도록 상시적인 모니터링이 가능해야 합니다.

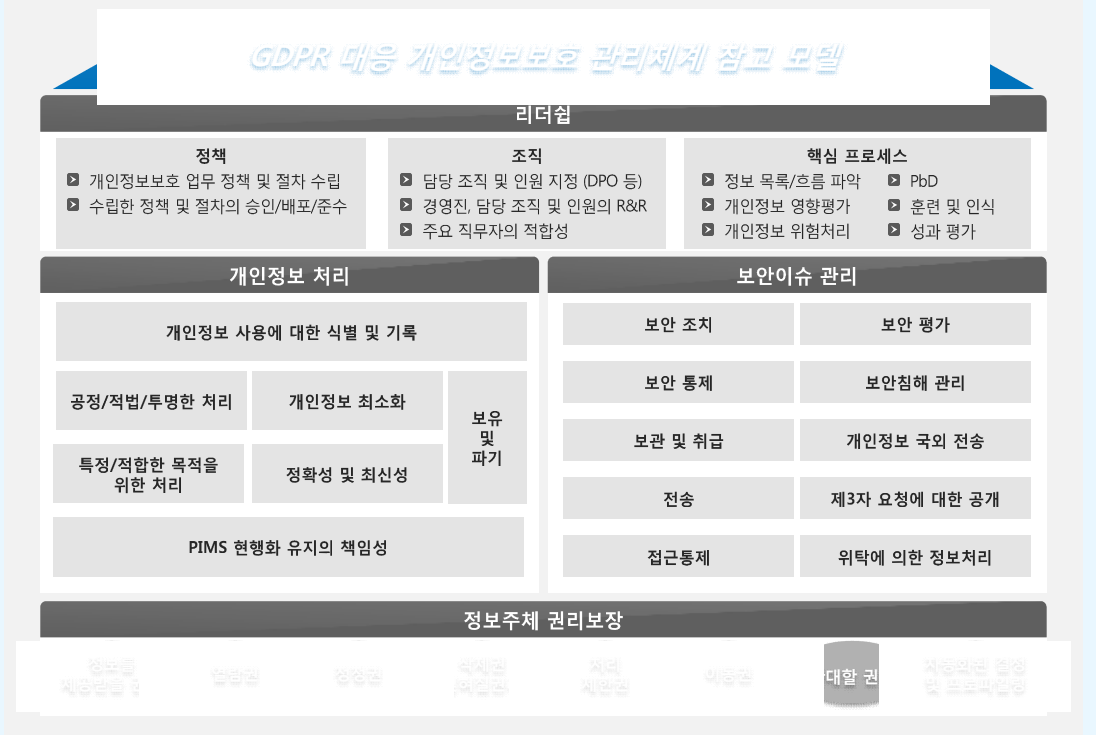
3.5 GDPR 전반의 요구사항에 대응 할 수 있는 자체 GDPR 대응 체계를 마련하십시오.

- GDPR 전반의 요구사항을 포함한 리더십, 개인정보 처리 관리, 보안이슈 관리, 정보주체 권리보장 방안 등이 필수 요소로 포함된 자체 GDPR 대응 체계를 마련해야 합니다.

- GDPR을 제대로 대응하기 위해서는 우선 GDPR의 명확한 이해 하에 조직 영향도를 파악한 후 효율적으로 대응하기 위한 조직 내부의 체계 정비가 선행되어야 합니다. 이러한 체계로는 GDPR 전반에 대한 리더십, 개인정보 처리 관리, 보안이슈 관리, 정보주체 권리보장 방안 등이 있습니다.

- 컨트롤러와 프로세서 입장에서 반드시 준수해야 하는 요소를 명확히 인지하고 이를 내부 관리체계 안에 반영시켜야합니다.

참 고



GDPR 대응 개인정보보호 관리체계 참고 모델 (BS10012:2017 내용 참조)

3.6 조직 특성에 맞는 다양한 보안이슈를 관리하십시오.

- 최신 기술, 구현 비용 및 개인정보 처리 성격, 범위, 상황 및 목적을 고려하여 가명화, 암호화 등 적절한 보안조치를 규정해야 합니다.

- 또한 보안 통제의 세부 사항 및 구현에 따라 개인정보 종류, 위험도 등을 고려하여 적절한 보안 조치를 구현해야 합니다.

- 저장·취급 및 전송에 안전성을 보장하고 보안 평가에 따른 접근 통제를 시행하십시오.

- 유사시 감독기구에 통보를 위해 (침해 인지후 72시간 내 통보) 보안침해 관리 관련한 제반 사항(발생배경, 조치사항, 시사점 등)을 평가하고 이를 관리 및 문서화하십시오.

▪ 제3자 요청에 대한 공개(법적근거, 개인정보 최소화, 기록유지 등) 및 위탁에 의한 정보처리(프로세서 선정시 유의사항 등)에 필요한 사항들을 준수하십시오.

참 고

컨트롤러 및 프로세서의 주요 준수 필요사항

■ 컨트롤러/프로세서 공통

① 개인정보 처리활동 기록 (종업원 250명 이상 기업 등)

② DPO 지정

③ EU 내 설립되지 않은 컨트롤러/프로세서의 경우 EU 역내 대리인 지정

④ 개인정보 침해 인지시 정보주체 통지 의무 (컨트롤러는 감독기구, 프로세서는 컨트롤러에게)

■ 컨트롤러

① GDPR 준수를 입증할 수 있는 적절한 기술적/조직적 조치

② 프로세서에 대해 구체적인 법적 의무를 부과 (예: 개인정보 처리활동 기록)

③ Data Protection by Design and Default

④ 개인정보영향평가 (Data Protection Impact Assessment)

⑤ 행동강령/인증제도 이용 (가능 시)

■ 프로세서

① 컨트롤러의 문서화된 지시사항에 의한 처리

② 개인정보 처리의 보안을 위해 요구되는 모든 조치 강구

③ 컨트롤러의 정보주체 권리 보장을 위해 필요한 조치 지원 활동

④ 컨트롤러와 관계 종료 시 컨트롤러 선택에 따라 개인정보 반환 또는 파기

⑤ GDPR 준수여부를 입증하기 위해 필요한 모든 정보를 컨트롤러에 제공

꼭 알아두기

[개인정보 처리 모니터링 필요사항]

■ 공정하고 적법하며 투명한 처리: 처리되기 전 법적 근거가 명확하게 확인될 수 있도록 해야 합니다(개인정보의 수집 및 처리, 개인정보의 기록(통지 및 진술 등), 개인정보의 타이밍, 개인정보의 접근 가능성, 제 3자로부터 수집).

■ 특정하고 적합한 목적을 위한 처리: 특정 목적으로만 획득되도록 보장해야 합니다(처리의 근거, 호환되지 않는 목적의 동의, 아동의 개인정보 처리, 공유 개인정보, 개인정보 매칭).

■ 개인정보 최소화 원칙에 따른 적절성 및 관련성: 과도하지 않아야 합니다.

■ 개인정보 정확성: 정확하고 필요한 경우 최신성을 유지해야 합니다.

■ 개인정보 보유 및 파기: 필요 이상 보관하지 않도록 보장해야 합니다.

관련 조문 및 근거

- 제4조 2항(개인정보 처리의 정의)
- 제5조(개인정보 처리 관련 원칙)
- 제6조(개인정보 처리의 적법성)
- 제9조(민감정보의 처리)
- 제33조(감독기구에 대한 개인정보 유출 통지)
- 전문 제52조
- 전문 제81조
- 전문 제91조
- 전문 제94조

Ⅲ. 기업 책임성 강화

1. Data Protection by Design and Default

Check List

[Data Protection by Design]
- 조직 내 IT 개발 절차를 확인하십시오.
- 개발 절차 내 적절한 기술 및 관리 조치를 채택하고 시행하십시오.

[Data Protection by Default]
- 어플리케이션·제품·서비스의 기본 설정이 프라이버시 친화적인지 검토하고 보완하십시오.

[Data Protection by Design]

1.1 조직 내 IT 개발 절차를 확인하십시오.

▪ 개인정보 처리에 기반하거나 업무를 위해 개인정보를 처리하는 어플리케이션, 서비스, 제품을 개발, 디자인, 선택 및 이용하는 모든 과정에서 개인정보 보호를 위한 적절한 기술적·조직적 조치가 강구되어야 합니다. 이를 위해 우선 조직 내에서 IT 기획·개발·검수 절차와 이 과정에서 고려하거나 검토하는 사항들을 확인하십시오.

1.2 개발 절차 내 적절한 기술 및 관리 조치를 채택하고 시행하십시오.

▪ 컨트롤러는 IT 개발 과정에서 아래의 사항을 고려하여 적절한 기술적·조직적 조치(appropriate technical and organizational measure)를 반영해야 합니다. 이와 같은 사항들은 개인정보 처리 수단을 결정한 시점과 처리 당시 시점에서 모두 고려되어야 합니다.

① 개인정보 처리의 최신 기술 수준(state of the art) : 벤치마킹이나, 기술적 솔루션의 도입 검토 혹은 조직적 관리 체계의 수립 등 개인정보 수집 단계부터 개인정보 처리를 위한 다양한 최신 기술을 고려해야 합니다.

② 실행 비용(cost of implementation) : 단순한 비용 및 이익 분석을 넘어 비례원칙에 따라 일정 수준 이상의 실행 비용이 수반되어야 합니다.

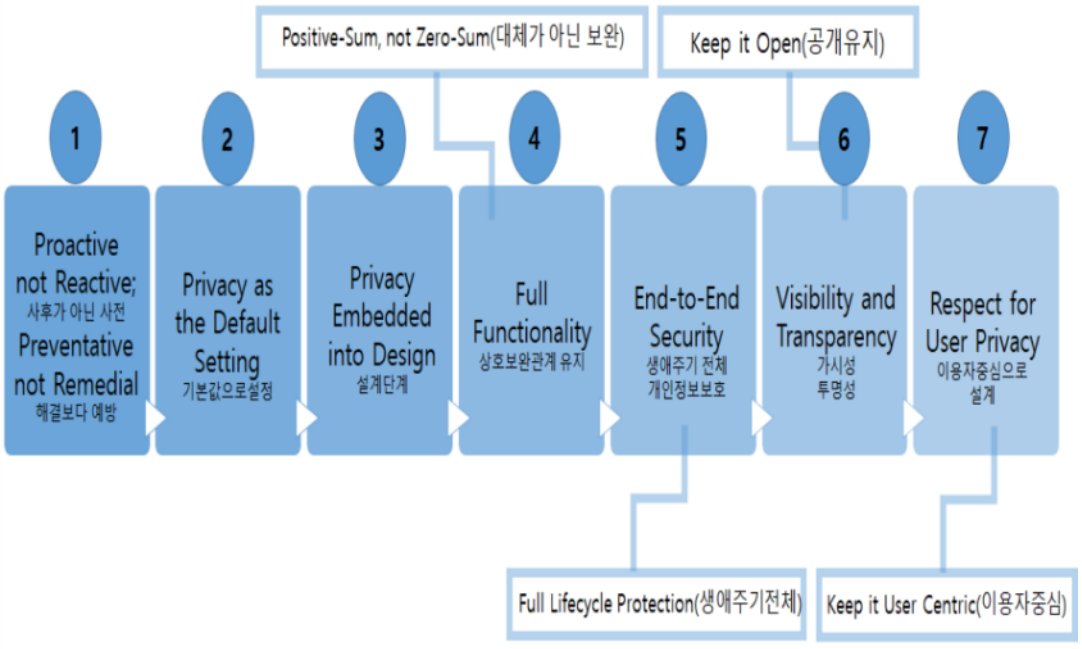
③ 개인정보 처리의 성격·범위·상황 : 개인정보 처리의 본질적 특성, 정보처리 규모나 정보주체의 수, 조직 및 기술적 환경의 범위, 여러 가지 데이터의 결합에 따라 신규 맥락 생성 가능성 등을 고려해야 합니다.

④ 개인정보 처리의 목적 : 개인정보는 목적을 고려하여 반드시 필요한 범위에서 최소한으로 처리되도록 해야 합니다.

⑤ 개인정보 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성, 중대성, 위험성 : 개인정보 처리로 인해 정보주체의 권리, 자유, 이익에 대해 잠재적으로 부정적인 영향을 미칠 수 없도록 해야 합니다.

▪ 적절한 기술적·조직적 조치로는 가명화(pseudonymisation), 개인정보처리의 최소화(data minimisation) 등이 있습니다. 또한 GDPR의 요구 사항을 준수하기 위해 개인정보 처리 과정 내에 필수적인 보호조치(safeguard)를 통합하고 정보주체의 권리를 보장해야 하는 방식으로 실행되어야 합니다.

< Data Protection by Design) 7원칙 >



참 고

■ Data Protection by Design 7원칙 : 1990년에 캐나다 온타리오 주의 정보 및 프라이버시 보호 위원 앤카부키안(Ann Cavoukian) 박사가 처음 제안한 것으로 설계(design) 단계에서부터 기술적으로 프라이버시를 보호하는 구조의 구축을 추진하는 것

① 사후적이 아닌 사전적 대비, 문제점을 고치는 것이 아니라 예방(Proactive not Reactive; Preventative not Remedial) : 프라이버시의 구제책을 고려하는 것이 아니라 예방책을 고려

② 프라이버시 보호를 기본값으로 설정(Data Protection as the Default Setting) : 기본 설정 상태의 시스템이나 비즈니스 프로세스에서 프라이버시를 보호

③ 계획에 포함된 프라이버시(Privacy Embedded into Design) : 설계 단계에서부터 시스템이나 비즈니스 프로세스에 프라이버시 대책을 포함

④ 포괄적 기능성 보장, 상호 대체 관계가 아닌 상호 보완 관계(Full Functionality - Positive-Sum, not Zero-Sum) : 제로섬이 아니라 포지티브 섬이어야 하는 것은 보안 대책 등과 프라이버시 보호는 상충 내지 대립(Trade-off) 되어서는 안 되고 상생 즉 상호 상생(Win-Win)의 관계

⑤ 시작에서 끝까지 보완 - 전체 수명주기(life cycle)의 보호(End-to-End Security - Full Lifestyle Protection) : 최초부터 최후까지 데이터 생애주기 전체에서 프라이버시 보호

⑥ 가시성과 투명성 - 항상 공개(Visibility and Transparency - Keep it Open) : 프라이버시 대책은 모든 이해관계인으로부터 가시적이고 투명해야 함

⑦ 개인의 프라이버시 존중 - 이용자 중심의 설계와 운영(Respect for User Privacy - Keep it User - Centric) : 시스템이나 비즈니스 프로세스의 설계자, 관리자는 이용자의 프라이버시를 최대한 존중

[Data Protection by Default]

1.3. 어플리케이션·제품·서비스의 기본 설정이 프라이버시 친화적인지 검토하고 보완하십시오.

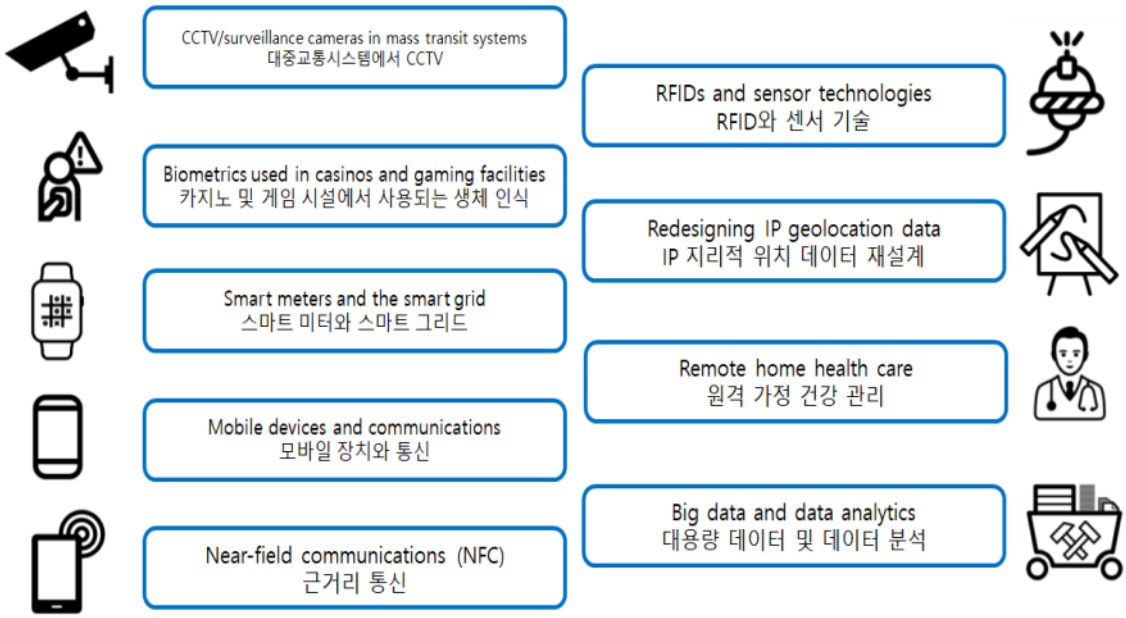
▪ 개인정보가 처리되는 제품·서비스·어플리케이션의 기본 설정은 특정 개인정보 처리 목적을 위한 최소한의 범위에서 개인정보가 활용되도록 이루어져야 합니다. 이는 고객이 새로운 제품이나 서비스를 구매하여 이용하는 경우, 혹은 이미 구입한 제품이나 서비스에 새로운 기능이 추가되는 경우 사용자

측에서 별도로 수동 설정이나 조치를 하지 않더라도 엄격한 수준의 개인정보 설정이 자동으로 적용될 수 있도록 조치해야 하는 것을 의미합니다.

※ 예를 들어, 소셜 미디어 서비스를 제공하면서 위치를 기반으로 서비스가 추가되었다고 하더라도 업데이트시 해당 기능이 자동으로 적용되어서는 안 됩니다.

▪ 따라서, 개인정보가 처리되는 조직의 어플리케이션·제품·서비스의 기본 설정(default)을 확인하고 동 설정이 프라이버시 친화적인지 검토하십시오. 만약 프라이버시 친화적이지 않다면 해당 값의 기본 설정을 프라이버시 친화적으로 변경하는 추가 개발에 착수하여 해당 어플리케이션·제품·서비스를 업데이트 해야합니다.
  - 특히 대중교통 시스템, 위치기반서비스, 센서기술, 원격의료, 대용량 데이터 분석 분야 등의 주요 어플리케이션은 검토가 필요한 분야라고 할 수 있습니다.

< 어플리케이션 9대 주요 영역 >



출처 : IT Governance Ltd 2017

▪ 또한, 기본 설정이 개별의 특정한 개인정보 처리 목적에 필요한 개인정보만 처리되는 것을 보장하기 위해 적절한 기술적·조직적 조치를 이행해야 합니다. 이러한 조치를 위해서는 아래의 사항을 고려해야 합니다.

① 수집되는 개인정보의 양(amount)
② 개인정보 처리의 범위
③ 개인정보 보유 기간
④ 개인정보에 대한 접근 가능성(accessibility)

- Data Protection by Design and Default 의 원칙은 공개 입찰(public tenders) 상황에서도 고려되어야 합니다. 이는 제품 및 소프트웨어를 자체적으로 생산하는 경우 외에 아웃소싱이나 외부 발주의 경우에도 지켜져야 함을 의미합니다.

꼭 알아두기

■ 적절한 기술적·조직적 조치(전문 제78조)
① 내부 정책을 수립해야 함
② 디자인 및 디폴트에 개인정보보호 원칙을 충족하는 조치를 실행해야 함
③ 동 조치는 아래와 같은 사항을 포함할 수 있음
- 개인정보 처리의 최소화
- 가능한 빠른 시점의 개인정보 가명화(pseudonymisation)
- 개인정보 처리 및 기능 관련 투명성의 확보
- 정보주체가 개인정보 처리를 감시할 수 있도록 허용
- 컨트롤러의 보안 사양(security features) 개발 및 향상 가능 조치

관련 조문 및 근거

■ 제25조(Data Protection by Design and Default)
■ 전문 제78조

2. 개인정보영향평가 (DPIA)

Check List

■ 우선 영향평가 실시 요건 및 방법에 대해서 인지하십시오.

① GDPR은 "자연인의 권리 및 자유에 대한 고위험을 초래할 가능성이 있을 때" ("likely to result in a high risk to the rights and freedoms of natural persons") 만 영향평가를 요구한다(법 제35조 제1항).

② 한 번의 평가로 유사한 복수의 처리작업을 일괄적으로 해결할 수 있다. ("a single assessment may address a set of similar processing operations that present similar high risks")

■ 영향평가를 의무적으로 수행해야 하는 경우인지 파악하십시오.

① 영향평가가 의무적인 경우는 "고위험 초래 가능성" 이 있을 때이다.

② 영향평가가 필요 없는 경우는 처리로 인한 높은 위험 발생 가능성이 없거나, 이미 승인되었거나, 법적 근거가 있는 경우 등이다.

■ (의무사항에 해당할 경우)개인정보 처리가 이루어지기 전에 절차에 따라 영향평가를 수행하십시오.

① 영향평가는 개인정보처리 전에 해야 하며, 처리작업의 기획단계 중 가장 일찍 시작하여야 한다.

② 컨트롤러는 DPO, 프로세서의 조언과 조력을 받아(The data controller, with the DPO and the data processor) 영향평가 실시에 책임을 져야 한다.

③ 영향평가는 예정처리작업 및 처리 목적, 필요성 및 비례성의 원칙에 대한 평가, 정보주체 권리 및 자유에 대한 위험평가 등을 고려해야한다.

④ 영향평가 결과는 공개(Publishing) 해야 하며 감독기구에 사전 협의했을 때는 해당 감독기구에 제공하여야 한다.

■ 감독기구와의 협의가 필요한 경우를 파악하십시오.

① 위험을 완화하고자 하는 컨트롤러의 조치가 부재한 경우

② 해당 처리가 고위험을 초래할 수 있는 경우

2.1 개인정보영향평가 실시 요건 및 방법에 대해서 인지하십시오.

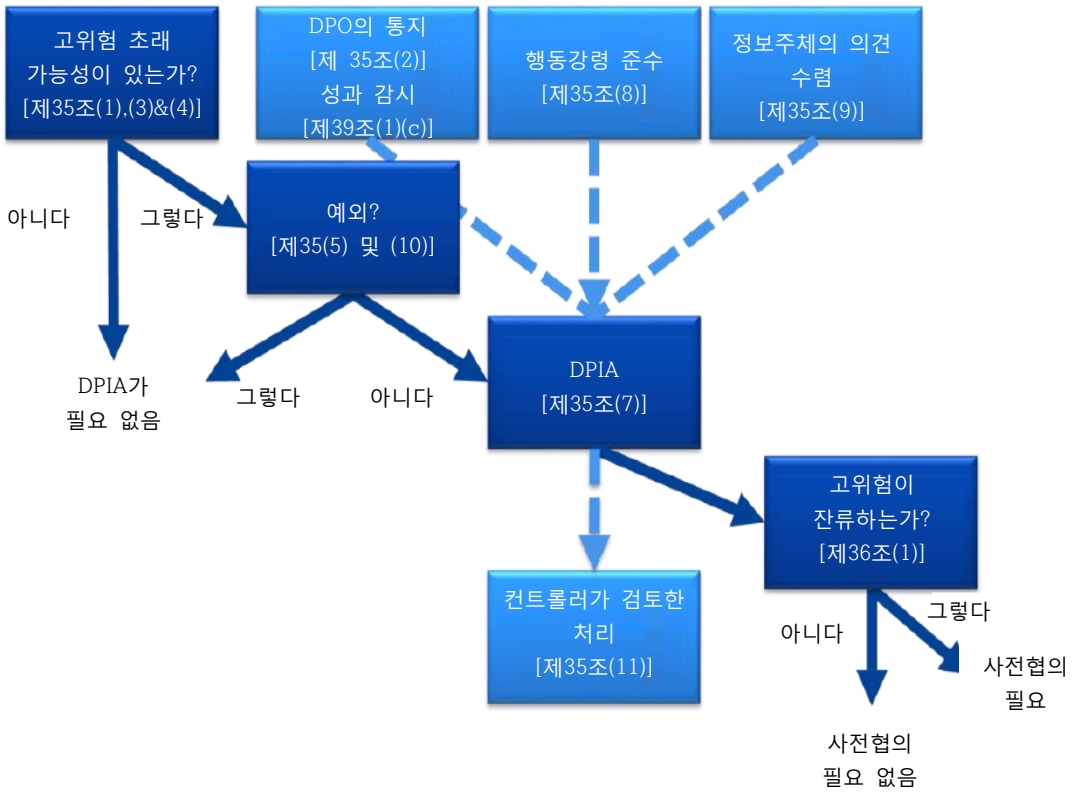
▪ GDPR은 "자연인의 권리 및 자유에 대한 고위험을 초래할 가능성이 있을 때"만 영향평가를 요구하고 있습니다.

▪ 한 번의 평가로 유사한 복수의 처리작업을 일괄적으로 해결할 수 있습니다.

- 이것은 동일한 목적으로 동일한 종류의 정보를 수집하기 위해 유사한 기술을 이용하는 경우를 의미할 수도 있습니다.

☞ **(예시)** 각자 유사한 CCTV 시스템을 설치하는 지방자치단체들이 각자의 별도 컨트롤러들에 의한 처리에 관해 집단적으로 한 번의 영향평가를 실시하거나, 철도 운영자(단일 컨트롤러)가 모든 기차역들의 비디오 감시에 관해 하나의 영향평가를 실시하는 경우

< GDPR에서의 개인정보영향평가 수행단계 흐름도>



2.2 영향평가를 의무적으로 수행해야 하는 경우를 파악하십시오.

▪ 개인정보 영향평가가 특히 요구되는 경우는 GDPR 제35조 제3항에 명시되어 있으며, 고위험(High risk)을 초래할 가능성은 아래와 같습니다.

① 프로파일링을 포함한 자동화된 처리에 근거한 자연인에 대한 체계적이고 광범위한 평가이며, 해당 평가에 기반한 결정이 해당 정보주체에게 법적 효력을 미치거나 이와 유사하게 중대한(significantly) 영향을 미치는 경우

② 민감정보(제9조 제1항) 또는 유죄 판결 및 형사범죄에 대한 대규모 처리(제10조)를 하는 경우

③ 공개적으로 접근 가능한 장소(publicly accessible areas)에 대한 대규모의 체계적인 모니터링(예: CCTV)

※ 고위험 초래할 가능성이 있는 개인정보 처리과정에서의 기준 9가지

① **평가 또는 평점:** 특히 정보주체의 업무성과, 경제적 여건, 건강, 개인적 취향이나 관심, 신뢰도나 자세, 위치나 이동(전문 제 71·91조)으로부터 작성하는 프로필이나 예측을 포함합니다.

☞ **(예시)** 은행이 그 고객을 신용조회 데이터베이스를 통해 선별하는 경우, 생명공학 기업이 질병/건강 위험의 측정 및 예측을 위해 유전자 검사를 실시하는 경우, 또는 기업이 자신의 웹사이트의 이용이나 검색 활동에 기초하여 행동 프로필이나 마케팅 프로필을 작성하는 경우 등

② **법적 효과 또는 비슷한 다른 중요한 효과를 지닌 자동 의사결정**: (법 제35조 제3항 (a)호) 개인정보 처리 알고리즘이 개인에 대한 배격이나 차별로 이어질 수 있는 경우이며, 개인에 대한 영향이 적거나 없는 처리는 이 특정 기준에 해당하지 않습니다.

☞ **(예시)** 온라인 광고가 여성보다 남성에게 보다 높은 임금의 직업 광고를 추천하는 경우 및 흑인들에게는 저렴한 상품을 집중적으로 보여주는 경우 등

③ **시스템을 이용한 감시**: (법 제35조 제3항 (c)호) 이 유형의 감시가 기준에 포함되는 이유는 누가 자신의 정보를 수집하는지, 그 정보가 어떻게 이용될 지를 정보주체가 모를 수 있는 상황에서 개인정보가 수집되기 때문입니다. 또한, 개인이 대중이 흔히 오가는 장소(또는 공공 이용 장소)에서 그런 처리의 대상이 되는 것을 피하는 것이 불가능할 수도 있습니다.

④ **민감한 정보**: 이것은 형사재판이나 범죄에 관한 정보뿐 아니라 제9조에 규정된 특별 부류의 정보(예를 들어, 개인의 정치적 견해에 관한 정보 등)도 포함합니다.

☞ **(예시)** 일반병원이 환자의 의료기록을 보관하는 경우, 심부름 센터 등이 범죄자의 정보를 보관하는 경우

⑤ **대규모로 처리하는 정보**: 무엇이 대규모에 해당하는지에 대해 전문 제91호에 약간의 지침은 제시되어 있지만, GDPR은 이에 대한 정의를 하지 않고 있습니다. 제29조 작업반은 특히 다음 요소들을 대규모로 실시된 처리인지 여부를 결정할 때 고려하도록 권고하고 있습니다.

- 관련 정보주체의 수
- 처리하는 정보의 양 또는 서로 다른 정보 항목들의 범위
- 정보 처리 활동의 기간 또는 영속성
- 처리 활동의 지리적 범위

⑥ **연계되거나 결합된 일단의 정보들:** 예를 들어, 다른 목적을 위해 또는 다른 컨트롤러들에 의해 실시된 둘 이상의 정보 처리 작업들을 통해 얻은 정보들을 정보주체의 합리적인 예상을 초과하는 방식으로 연계하거나 결합하는 것들이 있습니다.

⑦ 취약한 정보주체에 관한 정보(전문 제75호): 이 유형의 정보의 처리는 정보주체와 컨트롤러간의 증대된 힘의 불균형 즉 개인이 자신의 정보에 대한 처리를 찬성하거나 반대할 능력이 없다는 점 때문에 영향평가가 요구될 수 있습니다. (아동, 정신질환이 있는 사람, 난민, 노인, 환자, 또는 정보주체와 컨트롤러간의 지위 관계의 불균형이 있는 모든 경우도 포함합니다.)

☞ **(예시)** 인적자원 관리와 연계하여 고용주가 처리하는 종업원의 개인정보

⑧ **기술적 기법이나 구조적 기법을 혁신적으로 변경하거나 적용하는 경우:** 물리적 접근 통제의 개선을 위해 지문이나 안면인식을 결합하여 사용하는 것 등이 이런 기법에 속합니다. GDPR은 새로운 기술의 사용은 개인정보영향평가 실시의 필요를 촉발할 수 있다고 명시합니다.(제35조 제1항 및 전문 제89·91조) 왜냐하면 그런 기술의 이용은 새로운 형태의 정보 수집 및 이용을 내포할 수 있으며 개인의 권리 및 자유에 대한 높은 위험을 수반할 수 있기 때문입니다.

☞ **(예시)** "사물인터넷" 관련 기술 적용은 개인의 일상생활 및 사생활에 중대한 영향을 줄 수 있는 경우

⑨ **처리 자체가 "정보주체의 권리 행사나 서비스 이용이나 계약을 방해" 하는 경우(제 22조 및 전문 제91호):** 이것은 공공장소에서 실시되며 행인이 피할 수 없는 처리, 또는 정보주체의 서비스 접근이나 계약 체결을 허락, 수정, 거부하기 위한 처리를 포함합니다.

☞ **(예시)** 은행이 대출 승인을 결정하기 위해 고객을 신용조회 데이터베이스를 통해 심사하는 경우

▪ 개인정보 영향평가가 필요 없는 경우는 처리로 인한 높은 위험 발생

가능성이 없거나, 이미 승인되었거나, 법적 근거가 있는 경우입니다.

① 처리의 성격, 범위, 내용 및 목적이 영향평가가 이미 실시된 처리와 매우 유사한 때는 해당 영향평가 결과를 이용할 수 있습니다(법 제35조 제1항)

② 처리가 EU나 회원국 법에 법적 근거가 있으며 최초의 영향평가 실시의 의무가 없다고 진술한 경우, 법으로 특정 처리작업을 규제하는 경우, 그리고 법적 근거 마련을 위해 GDPR 표준에 따른 영향평가가 이미 실시된 경우(법 제35조 제10항)

③ 처리가 영향평가가 요구되지 않는 임의사항 목록(감독기구가 수립한)에 포함된 경우(법 제35조 제5항). 그런 목록에는 이 감독기구가 특히 지침, 특별 결정이나 승인, 면제, 준수 규정 등을 통해 규정한 조건에 부합하는 처리 활동이 포함될 수도 있습니다. 그런 경우에는, 소관 감독기구의 재평가를 단서로 영향평가가 요구되지 않지만, 그 처리가 목록에 규정된 관련 절차의 범위 내에 정확히 속하며 계속적으로 관련 요건을 완전히 충족시킬 때에만 그러합니다.

▪ 기본적으로 영향평가는 GDPR 발효이후 개시된 처리업무에 적용되나, GDPR 시행('18.5)전 기존의 처리업무라도 시행이후 새로 생성되거나 크게 변화된 처리에는 요구됩니다.

① 제29조 작업반은 2018년 5월 전에 이미 진행 중이던 처리업무에도 영향평가를 실시하기를 강력히 권고합니다. 또한 필요하다면, "관리자는 적어도 처리업무로 인한 위험의 변화가 있을 때에는 영향평가에 부합하여 처리가 이루어지고 있는지 평가하는 재검토를 실시해야합니다"(법 제35조 제11항)).

② 새로운 기술이 사용되거나 개인정보가 다른 목적으로 이용되는 등, GDPR 시행 이후 처리업무에 중대한 변화가 생긴 경우에는 사실상 새로운 정보처리로 보고 영향평가 대상이 됩니다. 아울러 처리업무에 의해 제기되는 위험의 변화가 있는 때에는 확실히 재검토되어야 합니다.

③ 위험은 처리작업의 요소(정보, 지원 자산, 위험의 원인, 잠재적 영향, 기능 등) 중 하나의 변화의 결과 또는 처리 내용(목적, 기능 등)의 변화로 인해

바뀔 수 있어 새로운 취약점이 발생할 수 있습니다. 따라서 영향평가의 수정은 지속적 개선 및 보호 수준을 유지하기 위해서도 중요합니다.

④ 아울러, 자동화된 의사 결정의 영향이 더 중대해졌거나, 새로운 부류의 자연인들이 차별에 노출되거나 EU를 탈퇴한 국가에 있는 수령인에게 정보를 전송하려고 하는 경우처럼 처리 활동에 관한 조직 및 사회적 맥락이 변경된 경우에도 필요합니다.

2.3 (의무사항에 해당할 경우)개인정보 처리가 이루어지기 전에 개인정보 영향평가를 수행하십시오.

▪ 영향평가는 개인정보처리 전에 해야 하며, 처리작업의 기획단계 중 가장 일찍 시작하여야 합니다.

① 개인정보영향평가는 “처리 전”에 해야 하며(법 제35조 제1항 및 제35조 제10항, 전문 제90조 및 제93조), 이것은 Data Protection by Design and Default 설계 원칙과 일치합니다(제25조 및 전문 제78조).

② 처리가 실제적으로 개시된 후에도 업데이트될 필요가 있다는 사실을 핑계로 개인정보영향평가를 지연하거나 실시하지 않는 것은 타당하지 않습니다. 개인정보영향평가는 지속적 과정이며, 변화의 영향을 받는 동적인 처리작업입니다.

▪ 컨트롤러는 DPO, 프로세서의 조언과 조력을 받아 영향평가 실시에 책임을 져야 합니다.

① 개인정보영향평가는 조직 내외의 다른 사람에 의해 실시될 수 있지만 그 과제에 대한 최종 책임은 컨트롤러에게 있습니다(법 제35조 제2항),

- 컨트롤러는 DPO의 조언을 구해야 하고 이 조언 및 그에 기초한 결정은 개인정보영향평가 내에 기록해야 하며, DPO는 개인정보영향평가의 실시에 대한 감시도 해야 합니다(법 제39조 제1항 (c)호).

- 처리의 전부 또는 일부가 프로세서에 의해 실시되는 경우에는 프로세서는

컨트롤러의 개인정보영향평가 수행을 보조하며 모든 필요한 정보를 제공해야 합니다.

- 컨트롤러는 정보주체나 그 대표자의 의견을 구해야 합니다(법 제35조 제9항).

☞ **(예시)** 의견을 구하는 다양한 수단으로 처리업무의 목적 및 수단에 관한 내부나 외부의 연구, 직원 대표나 노동조합에 대한 공식 질의, 정보 컨트롤러의 미래 고객들에게 보내는 설문조사 등

- 컨트롤러의 최종 결정이 정보주체의 의견과 다른 경우에는 계속 진행하거나 중단하는 이유를 기록해야 합니다.

- 컨트롤러가 정보주체의 의견을 구하는 것이 적절하지 않다고 결정하는 경우에는 그 이유의 근거를 기록해야 합니다.

② 컨트롤러는 내부 정책, 절차 및 규칙에 따라 다음과 같이 다른 특정 역할 및 책임을 정의해야 합니다.

- 특정 사업부서가 개인정보영향평가의 실시를 제안하는 경우에는 그 해당 부서에서 개인정보영향평가에 대한 조언을 제공해야 하며 또한 영향평가 절차에 관여해야 합니다.

- 가급적 다른 직종의 전문가(변호사, 기술자, 보안 전문가, 사회학자, 윤리학자 등)의 조언을 구하는 것이 바람직합니다.

- 프로세서의 역할 및 책임은 계약으로 정의해야 합니다. 또한 개인정보영향평가는 프로세서의 도움을 얻어 실시해야 하며, 처리의 성격 및 프로세서가 이용할 수 있는 정보를 고려해야 합니다(법 제28조 제3항 (f)호).

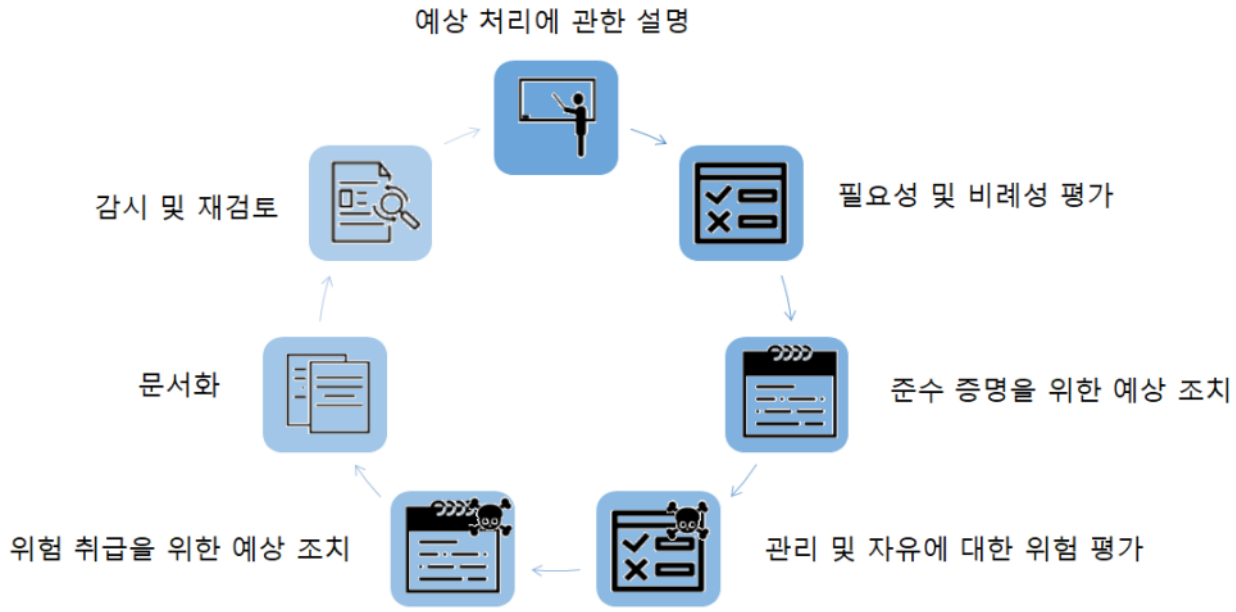
- DPO는 특정 처리업무에 관한 개인정보영향평가를 실시할 것을 컨트롤러에게 제안할 수 있고 방법론에 관해 이해관계자들을 지원해야 하며, 위험 평가의 수준 평가에 도움을 주어야 합니다. 또한 잔여 위험이 수용할만한지 평가하는 데에 도움을 주어야 하며, 컨트롤러 입장에 특유한 지식의 개발에도 기여

해야 합니다.

- 최고정보보안책임자(CISO) 또는 IT부서는 컨트롤러에 대한 지원을 제공해야 하며, 보안이나 업무상 필요에 따라 특정 처리작업에 관한 개인정보영향평가의 실시를 제안할 수 있습니다.

▪ 영향평가는 예정처리작업 및 처리목적, 필요성 및 비례성의 원칙 (과잉금지의 원칙, the proportionality consideration ; 기본권을 제한함으로서 달성되는 공익과 침해되는 사익을 비교하여 전자가 후자보다 월등하여야 한다는 원리)에 대한 평가, 정보주체 권리 및 자유에 대한 위험평가 등을 고려해야합니다.

< GDPR에서의 개인정보 영향평가 실시 절차 >



① GDPR은 개인정보영향평가의 최소한의 특성을 다음과 같이 규정하고 있습니다. (법 제35조 제7항, 전문 제84호 및 제90호)

- “예정 처리작업의 설명 및 처리의 목적”
- “처리의 필요 및 비례성의 원칙에 대한 평가”
- “정보주체의 권리 및 자유에 대한 위험의 평가”
- “위험의 취급 및 규칙 준수의 증명”

② 정보 처리작업의 영향을 평가할 때에는 행동강령의 준수(제40조)를

고려해야 합니다. 이것은 행동강령이 처리작업에 적합한 경우, 적절한 조치가 선택되었거나 취해졌다는 것을 증명하는 데에 도움이 될 수 있습니다.

③ GDPR은 위험 관리 구성요소(예를 들어 ISO 31000)와 중첩되는 여러 개인정보영향평가 구성요소들을 열거하고 있습니다. (전문 제90조)

- 맥락의 설정(Context Establishment) : “처리의 성격, 범위, 내용 및 목적과 위험의 출처를 검토한다.”
- 위험의 평가: “고위험의 개연성 및 심각성에 대해 평가한다.”
- 위험의 처리(Risk Treatment) : “위험을 완화”하며 “개인정보 보호를 확보”하며 “규칙 준수를 증명”한다.

④ GDPR의 개인정보영향평가 규정은 컨트롤러에게 기존의 업무 관행에 부합하도록 영향평가의 정확한 구조 및 형태를 결정할 융통성을 부여합니다.

- EU와 전 세계에는 이미 여러 기존의 절차들이 전문 제90조에 규정된 구성요소들을 반영하고 있습니다.
- 그러나 그 형태가 무엇이든 간에 개인정보영향평가는 컨트롤러가 위험을 다루는 조치를 취할 수 있게 해주는 진정한 위험 평가 수단입니다.

⑤ 제29조 작업반은 분야별 특화된 개인정보영향평가 체계의 개발을 권장합니다.

- 즉 개인정보영향평가가 특정 유형의 처리업무의 구체적 사항(예를 들어, 특정 유형의 정보, 기업 자산, 잠재적 영향, 위협, 조치)을 다룰 수 있게 되기 때문입니다.
- 이것은 개인정보영향평가가 특정 경제 부문에서 발생하거나 특정 기술을 이용할 때 또는 특정 유형의 처리작업을 수행할 때 발생하는 이슈들을 다룰 수 있다는 것을 의미합니다.

▪ 영향평가 결과는 공개(Publishing) 하는 것이 좋으며, 감독기구에 사전협의 했을 때는 해당 당국에 제공하여야 한다.

① 개인정보영향평가의 공개는 GDPR의 법적 요건은 아니며 컨트롤러의 재량사항입니다. 그러나 컨트롤러는 그들의 개인정보영향평가를 공개할지

검토해야 하며, 아니면 최소한 일부라도 공개할지를 검토해야 합니다.

- 공개의 목적은 신뢰 증대와 책임감 및 투명성을 증명하기 위함이므로 사회 구성원들이 영향을 받는 경우에는 개인정보영향평가를 공개하는 것이 좋습니다.

② 공개된 개인정보영향평가는 평가의 전체를 게재할 필요가 없으며, (특히 개인정보영향평가가 컨트롤러를 위한 보안 위험에 관한 구체적 정보를 제시할 수 있거나 또는 영업 비밀이나 상업적으로 민감한 정보를 누출할 수 있을 경우 등) 개인정보영향평가의 주요 결론의 요약만으로 구성할 수도 있습니다.

③ 개인정보영향평가가 높은 잔여 위험을 지닌 경우에는, 컨트롤러는 처리에 관하여 감독기구와 사전에 협의해야 합니다.(법 제36조 제3항 (e)호).

2.4 감독기구와의 협의가 필요한 경우를 파악하십시오.

▪ 위험을 완화하고자 하는 컨트롤러의 조치가 부재한 경우

① 정보주체의 권리 및 자유에 대한 위험을 평가하는 것과 이런 위험을 수용할만한 수준으로 줄이기 위해 예상되는 조치를 확정하는 것과 GDPR의 준수를 증명하는 것은 컨트롤러의 책임입니다(법 제35조 제7항, (c)호).

② 컨트롤러가 충분한 조치를 발견할 수 없는 모든 경우에는(즉 잔여 위험이 여전히 높을 때에는) 감독기구와의 협의가 필요합니다.

▪ 해당 처리가 고위험을 초래할 수 있는 경우

① 고위험의 예에는 정보주체가 극복할 수 없는 중대하거나 되돌릴 수 없는 결과에 직면하게 되거나 또는 위험이 발생할 것이 명백한 경우가 포함됩니다.

② 사회 보호 및 공중보건에 관한 처리를 포함한, 컨트롤러가 공익을 위해 수행한 과제의 성과를 파악하기 위해 실시한 처리에 관하여, 회원국 법이 컨트롤러에게 감독기구와 협의 또는 사전 승인을 받도록 규정한 모든 경우에는 컨트롤러가 필히 감독기구와 협의해야 합니다(법 제36조 제5

항).

꼭 알아두기

- 고위험 초래 가능성이 있는 개인정보를 취급하는 경우는 반드시 영향평가를 받아야 합니다.
- 고위험 초래 가능성 관련 EC에서 제시한 9개 가이드라인을 숙지하십시오.
- 영향평가는 개인정보 처리 단계 중에 가장 먼저 고려되고 실행되어야 합니다.
- 컨트롤러는 수행된 영향평가에 위험완화 조치가 미비 또는 부재한 경우 및 고위험 초래 가능성이 있는 경우에는 감독기구에 자문을 구해야 합니다.

관련 조문 및 근거

- 제35조(개인정보 영향평가)
- 제36조(사전 자문)
- 전문 제89~96조

3. DPO 임명

Check List

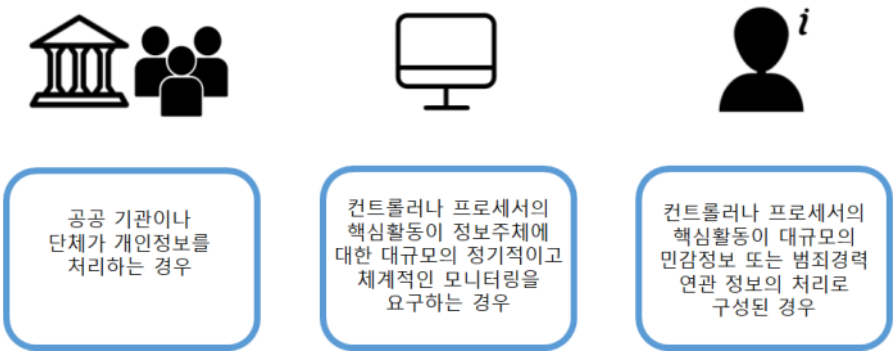
- 의무적으로 DPO를 지정해야 하는 경우를 확인하십시오.

① 공공 기관이나 단체가 개인정보를 처리하는 경우
② 컨트롤러나 프로세서의 핵심 활동이 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링을 요구하는 경우
③ 컨트롤러나 프로세서의 핵심 활동이 대규모의 민감정보 또는 범죄경력 연관 정보의 처리로 구성된 경우

- DPO 지정 시, 전문적 자질, 개인정보보호 법령에 대한 지식, 감독 기관과의 협업 경험, 관계자와의 커뮤니케이션 능력을 고려하십시오.
- DPO의 업무 독립성을 보장하고 이해의 충돌을 방지하십시오.

3.1 의무적으로 DPO를 지정해야 하는 경우를 확인하십시오.

< 의무적으로 DPO 지정해야 하는 경우 >



▪ DPO는 다음의 어느 하나에 해당하는 경우 지정 의무가 발생합니다.(법 제37조 제1항)

① 개인정보의 처리가 공공 기관이나 단체에 의해 수행되는 경우
② 컨트롤러나 프로세서의 핵심 활동이 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링을 요구하는 경우
③ 컨트롤러나 프로세서의 핵심 활동이 대규모의 민감정보 또는 범죄경력 관련 정보의 처리로 구성된 경우

▪ DPO 지정 요건을 이해하기 위해서는 “핵심 활동(core activities)”, “대규모의(on a large scale)”, “정기적이고 체계적인 모니터링” 등의 개념을 충분히 숙지해야 합니다. (자세한 사항은 WP29의 DPO가이드 라인 참조)

참 고

<핵심 활동> 의 예시

병원의 핵심적인 활동은 의료 서비스를 제공하는 것이며, 병원이 환자의 의료 기록과 같은 건강 개인정보를 처리하지 않고서는 안전하고 효율적인 건강관리를 제공할 수 없습니다. 그러므로 이런 개인정보 처리는 병원의 핵심적인 활동 중 하나인 것으로 간주되어야 하고 따라서 병원은 DPO를 지정해야 합니다.

보안 회사는 쇼핑센터 등 공적인 공간을 감시하며, 이 감시는 기업의 핵심적인 활동이고, 불가피하게 개인정보의 처리와 연계되어 있습니다. 따라서 이 기업 또한 DPO를 지정해야 합니다.

<대규모(LARGE SCALE)처리>의 예시

-정기적인 업무 과정에서 병원의 환자 개인정보 처리
-도시의 교통 시스템을 이용하는 개인들의 이동 개인정보 처리(교통 카드를 통한 추적 등)
-패스트푸드 체인 고객의 실시간 지리 위치 개인정보의 처리로서 통계 목적인 경우
-보험회사 또는 은행의 정기적인 사업 과정에서 고객 개인정보의 처리
-행동 양식에 따른 광고를 위한 검색 엔진의 개인정보 처리
-전화 또는 인터넷 서비스 제공업체의 개인정보(콘텐츠, 트래픽, 위치) 처리

<정기적이고 체계적인 모니터링>의 의미 및 예시

‘정기적인(regular)’는 다음의 하나 또는 그 이상을 의미합니다.

- 지속적으로 혹은 특정 기간 동안에 특정한 간격으로 발생
- 고정된 주기로 재발하거나 반복
- 지속적으로 혹은 주기적으로 발생

‘체계적인(systematic)’을 다음의 하나 또는 그 이상을 의미합니다.

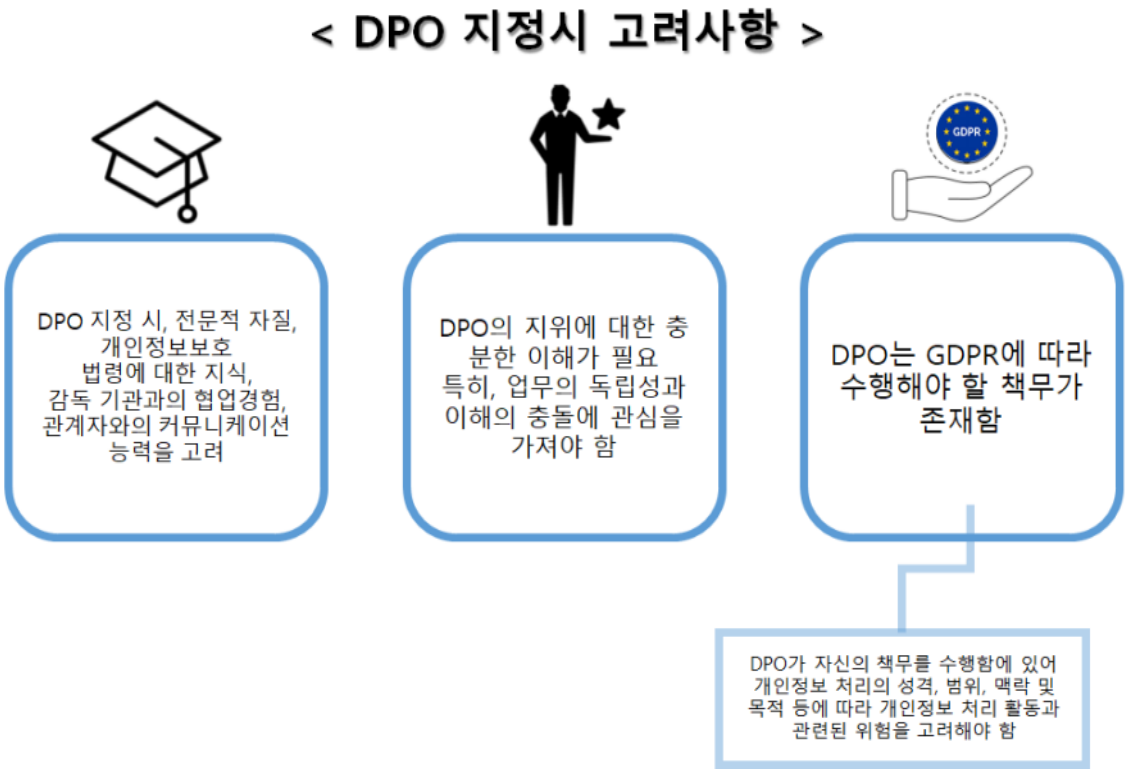
- 시스템에 의하여 발생하고 미리 예정되고, 조직화되거나 또는 규칙적인 경우
- 개인정보 수집을 위한 계획의 일환, 또는 전략의 일부로서 수행되는 경우

- 모바일 앱을 통한 위치 추적, 고객보상 프로그램, 행동 양식에 따른 광고
- 착용 형 기기(wearable device)를 통한 건강, 신체 및 의료 개인정보의 모니터링

▪ DPO를 지정하거나 또는 위 요건에 해당하지 않아 지정하지 않는 결정을 내린 경우, 그와 같은 결정을 내린 사유를 문서화 하는 것이 GDPR의 책임성 원칙에 따른 '문서화' 요건을 충족한 것으로 이해됩니다.

▪ 위의 요건에 해당하지 않더라도 DPO를 자발적으로 지정할 수 있습니다. 단, 자발적으로 DPO를 지정한 경우라도 DPO의 지정, 지위, 책무 등과 관련한 GDPR 제37~39조가 적용되므로 유의해야 합니다.

▪ DPO의 역할을 수행하지만, 지정에 따른 여러 법적 요구 사항으로부터 자유로워지려면 DPO와는 다른 명칭으로 담당자를 지정하거나 채용해야 합니다. 또한, 이와 같이 지정 또는 채용된 사람이 DPO가 아니라는 사실은 기업 내부, 감독 기관, 정보주체와의 커뮤니케이션 과정에서 명확히 드러나야 합니다.



3.2 DPO 지정 시, 전문적 자질, 개인정보보호 법령에 대한 지식, 감독 기관과의 협업 경험, 관계자와의 커뮤니케이션 능력을 고려하십시오.

- 전문적 자질(professional qualities)은 조직이 처리하는 개인정보의 양, 민감도, 복잡도 등에 상응해야 하지만 구체적으로 정의내릴 수 있는 개념은 아닙니다. 또한, 개인정보의 해외전송이 발생하는지에 따라 보다 높은 전문적 자질이 요구될 수도 있습니다.

- DPO가 갖추어야 하는 개인정보보호 법령에 대한 전문 지식(expertise)이 개인정보 보호 분야의 자격증의 취득이나, 박사학위 등 고학력이나 정보보호 분야에서 일정 기간 이상의 경력을 구체적으로 의미하는 것은 아닙니다. 그러나, 이런 사실들이 전문 지식을 보유한 DPO를 확보했다는 사실을 증명하는 것에 도움이 될 수 있습니다.

- DPO는 정보보호 감독기구와 협업한 경험을 갖추어야 합니다. 이는 사적으로 감독기구 종사자와 업무연락을 취할 수 있는 사회적 관계를 요구하는 것이 아닙니다. 정보보호 감독기구가 추구하는 정책적 목표를 이해하고 감독기구가 작동하는 메커니즘을 이해하여 감독기구와의 협업 과정에서 원활한 커뮤니케이션을 수행할 수 있는 능력이 필요하다는 것을 의미합니다.

- DPO는 조직 내부에서의 커뮤니케이션 뿐만 아니라, 감독기구 및 정보주체와도 커뮤니케이션을 수행합니다. 개인정보 처리로 인해 영향받는 다양한 관계자와의 커뮤니케이션을 수행해야 하기 때문에 커뮤니케이션 능력이 필수적으로 요구됩니다. 또한, 커뮤니케이션 능력은 유럽연합에서 일반적으로 사용되는 언어 구사능력이 요구됨을 의미합니다. DPO가 유럽연합의 언어를 직접 구사하지 못하는 경우, 조직은 전문적인 통역 자원을 DPO에게 지원해야 합니다.

3.3 DPO의 업무 독립성을 보장하고 이해의 충돌을 방지하십시오.

- DPO는 자신의 책무를 수행하는 것과 관련하여 컨트롤러나 프로세서로부터 어떠한 지시도 받지 않는 것이 보장되어야 합니다. 특히, DPO는 업무 수행과 관련하여 징계를 받거나 해고될 수 없습니다. 실제 직접적인 징계가 내려지지 않더라도, DPO의 활동과 관련하여 처벌의 가능성을 제시하는 경우에도

징계를 부과한 것으로 이해될 수 있어 주의를 요합니다.

- DPO는 GDPR이 정한 책무 외에 다른 업무를 수행할 수 있습니다. 이 때, 컨트롤러나 프로세서는 그와 같은 업무가 이해의 충돌(a conflict of interests)을 야기하지 않는 것을 보장해야 합니다. 예를 들어, DPO가 정보처리와 관련한 정책을 설정하는 내부 임직원인 경우 GDPR의 준수보다 비즈니스를 위한 정보처리의 효율성을 우선적으로 추구할 수 있으며, 이로 인해 이해의 충돌이 발생할 수 있습니다. 컨트롤러나 프로세서는 이와 같은 이해의 충돌이 발생하지 않도록 해야 합니다.

- 컨트롤러와 프로세서는 적절하고 적시적인 방법으로 DPO가 개인정보 보호와 관련한 모든 사안에 참여할 수 있다는 것을 보장해야 합니다. DPO가 GDPR에 규정된 그의 책무를 수행함에 있어 필요한 자원을 제공하고, 개인정보 처리활동에 접근할 수 있도록 지원해야 합니다. 또한, DPO가 전문 지식을 유지할 수 있도록 지원해야 합니다. DPO가 그의 책무를 효과적이고 효율적으로 이행하는데 필요한 경우라면 팀을 구성하는 방안도 적극적으로 검토되어야 합니다.

- DPO는 다음과 같은 책무를 수행해야 합니다. 단, 아래의 사항은 DPO의 최소 책무에 해당합니다. DPO가 자신의 책무를 수행함에 있어 개인정보 처리의 성격, 범위, 맥락 및 목적 등에 따라 개인정보 처리 활동과 관련된 위험을 고려해야 합니다. (법 제39조 제1항)

① 컨트롤러나 프로세서, 개인정보를 처리하는 임직원들에게 GDPR 및 유럽연합 회원국의 개인정보보호 규정에 따른 의무사항을 알리고 조언

② 개인정보의 보호와 관련하여 GDPR 및 유럽연합 회원국의 개인정보보호 규정, 개인정보보호와 관련한 컨트롤러 또는 프로세서의 정책 준수를 모니터링

③ 개인정보영향평가와 관련하여 요청받는 경우 조언을 제공하고, 영향평가에 따른 업무 수행을 모니터링

④ 감독기구와 협력

⑤ 사전 자문(제36조)에 규정된 사전 자문 절차의 이행 등, 개인정보 처리 관련 사안에 대해 감독기구와의 접촉 창구 역할을 수행

⑥ 기타, 적절한 경우 다른 사안에 대한 자문을 제공

▪ 특히, 개인정보 영향평가와 관련하여 DPO는 다음 사항에 대해 조언을 제시하도록 권고됩니다.

① 개인정보 영향평가를 수행할지 여부에 대한 결정
② 개인정보 영향평가를 수행할 때 따라야 할 방법론
③ 개인정보 영향평가를 내부에서 수행할지 또는 아웃소싱할지에 대한 결정
④ 정보주체의 권리와 이익에 대한 위험을 감소시키기 위해 적용해야 할 안전조치
⑤ 개인정보 영향평가가 적절히 수행되었는지에 대한 사후 평가

꼭 알아두기

- DPO 지정 요건에 해당하는 경우, DPO를 지정해야 합니다. 요건에 해당하지 않는 것으로 판단하여 미지정 하는 경우, 관련 사항을 문서화 하십시오.
- DPO를 지정할 때, 전문가로서의 자질, 전문적 지식, 감독기구와의 협업경험, 커뮤니케이션 능력 등을 고루 고려해야 합니다.
- DPO는 업무 수행에 있어 독립성이 보장되어야 합니다. 조직에서 다른 업무를 함께 수행하는 경우, 이익의 충돌이 발생해서는 안 됩니다.
- DPO는 GDPR에 규정된 최소한의 수행 업무를 부담하며, 기타 모든 개인정보 보호와 관련한 업무에 참여할 수 있어야 합니다.

관련 조문 및 근거

- 제35조(개인정보보호영향평가)
- 제36조(사전자문)
- 제37조(DPO의 지정)
- 제38조(DPO의 지위)
- 제39조(DPO의 책무)
- 전문 제97조

4. 개인정보 국외이전

Check List

■ 처리되는 개인정보를 식별하고 흐름을 파악하십시오. (정보의 흐름, 이전항목, 이전목적 등 국외이전에 관한 사실관계를 확인 등)

■ 국외이전에 적합한 메커니즘을 선정하십시오.

① 유럽경제지역(EEA) 외에도 EU 집행위원회에 의해 안전한 국가로 분류된 국가로 개인정보를 이전하는 경우에는 일반적으로 별도의 보호조치를 필요로 하지 않습니다. 개인정보를 미국으로 이전하는 경우, 이전받는 자가 미국의 Privacy Shield에 등록했는지 여부를 검토하십시오.

② 국외이전에 대한 표준계약이 채택 가능한 지 여부를 검토하십시오.

③ 그룹 내부로의 개인정보 이전이라면 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules)을 고려할 수 있습니다.

④ 조직의 업무와 관련된 승인된 행동강령(Code of Conduct) 및 인증제도(Certificate)를 고려하십시오.

■ 자사의 개인정보의 이전이 국외이전의 특정한 예외상황에 해당하는 지 확인하십시오.

4.1 처리되는 개인정보를 식별하고 흐름을 파악하십시오.

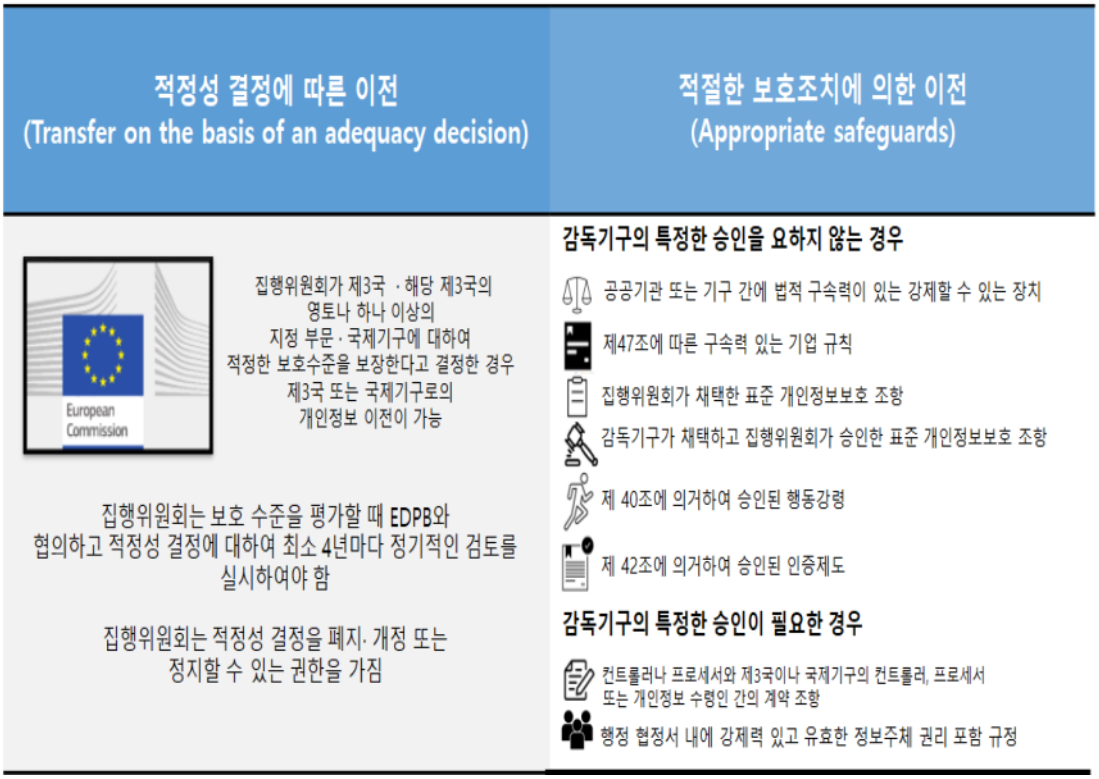
▪ 개인정보를 국외로 이전하기 위해서는 이전하는 정보의 항목, 이전하는 자, 이전받는 자, 이전받는 목적, 정보의 흐름, 적절한 안전조치 여부 등을 확인하십시오. 국외이전에는 이전하거나 받는 국가(또는 국제기구)에서 기타 제3국(또는 국제기구)로 개인정보를 이전하는 경우도 포함합니다 (Onward transfer).

▪ 컨트롤러와 프로세서가 현재 처리 중이거나 제3국(또는 국제기구)으로 이전 후에 처리예정인 개인정보는 GDPR의 규정에 조건을 준수하는 경우에만 이전이 가능합니다.

※ 28개의 EU 회원국 및 아이슬란드, 노르웨이, 리히텐슈타인으로 구성되는 EEA(European Economic Area)내부의 데이터 이전은 일반적으로 별도의 보호조치가 불필요합니다.

4.2 국외이전에 적합한 메커니즘을 선정하십시오.

< 개인정보 국외 이전 매커니즘 >



- GDPR상의 국외이전 메커니즘 : 1) 적정성 결정(Adequacy Decision), 2) 표준 계약(Standard Clauses), 3) 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules), 4) 승인된 행동강령(Code of Conduct) 및 인증 제도 (Certificate) 등이 있습니다.

- 적정성 결정에 따른 이전 : EEA 이외에도 EU에 의해 안전하다고 분류된 국가로의 이전에는 일반적으로 별도의 보호조치를 필요로 하지 않습니다.

※ 적절한 안전조치를 갖춘 국가:

Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, United States of America (총 12개국)

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm 에서 확인 가능합니다.

또한, 유럽 시민의 개인정보를 미국으로 이전하는 경우, 해당정보를 이전받는 자가 Privacy Shield에 등록된 경우 국외이전이 가능합니다.

※ Privacy Shield 등록여부는 https://www.privacyshield.gov/list 에서 확인할 수 있습니다.

▪ 적절한 안전조치에 의한 이전

① 표준계약 조항 : EU 집행위원회가 제공한 표준계약조항을 사용할 수 있습니다. 일부 국가의 경우 개인정보의 국외이전 시 표준계약조항에 대해 규제기관에 승인의무를 부과하고 있었습니다만, GDPR에서는 감독기구에 대한 승인 또는 신고절차가 폐지되었습니다.

② 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules) : 그룹 내부의 이전이라면 BCRs(Binding Corporate Rules)의 채택을 고려할 수 있습니다. 다국적 기업이 BCRs을 채택하고 EU 규제기관에 승인을 받는 경우, 개인정보 이전에 적절한 보호체계가 갖추어지지 않은 제3국에 위치한 그룹사로 이전하는 것이 가능합니다.

※ 이러한 절차 진행을 위해서는 EU 내 감독기구를 선정하고, EU 감독기구간의 협력절차 및 상호인증을 통해 기업의 BCRs이 승인을 받아야 합니다.

※ BCRs 명시사항

(a) 공동 경제활동에 관여하는 사업체 집단, 기업집단 및 각 구성원의 구조와 연락처

(b) 개인정보의 범주, 처리 유형과 목적, 관련 정보주체의 유형, 및 해당 제3국의 신원 등의 정보 이전 또는 이전 건 일체

(c) 내외부적으로 법적 구속력이 있는 특성

(d) 목적제한과 데이터 최소화, 보관기간 제한, 정보 품질, 설계 및 기본 설정에 의한 정보보호, 정보처리의 법적 근거, 특별한 유형의 개인정보

처리, 정보 보안 확보 대책 등의 일반정보보호 원칙 및 향후 기업 규칙의 구속을 받지 않는 기구에 대한 정보이전과 관련된 요건의 적용

(e) 제22조에 의거한 프로파일링 등 자동 처리만을 근거로 한 결정을 따르지 않을 권리, 제79조에 의거한 관할 감독기구 및 회원국 관할 법원에 민원을 제기할 권리, 그리고 의무적 기업 규칙 위반에 따른 구제 및 해당하는 경우 보상을 받을 권리가 포함된 개인정보 처리에 관한 정보주체의 권리 및 이 권리를 행사하기 위한 수단

(f) 유럽연합에서 정하지 않은 관련 회원국의 의무적 기업 규칙 위반에 대한 컨트롤러나 프로세서의 책임 인정. 컨트롤러나 프로세서는 해당 회원국이 피해를 유발한 사건에 대하여 책임이 없음을 증명할 경우에 한해 책임의 전부 또는 일부를 면할 수 있음

(g) 제13조 및 제14조(정보를 제공 받을 권리)에 더하여, 본 호의 (d), (e), (f)에 명시된 규정 등 의무적 기업 규칙에 관한 정보가 정보주체에 제공되는 방식

(h) 제37조에 의거하여 지정된 DPO 또는 교육 및 민원처리 감독을 비롯하여 집단 내에서 의무적 기업 규칙의 준수 여부를 감독하는 담당자 또는 주체의 업무

(i) 민원 절차

(j) 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단 내의 의무적 기업 규칙의 준수여부를 검증하기 위한 메커니즘. 이 같은 메커니즘은 정보보호 감사 및 정보주체의 권리 보호를 위한 시정조치를 보장할 방법을 포함해야 한다. 해당 검증 결과는 (h)에 언급된 개인이나 개체 및 기업 집단이나 그 사업을 총괄하는 이사회에게 전달해야 하고, 관할 감독기구의 요구가 있을 시 이를 제공해야함

(k) 규정의 변경사항을 보고 및 기록하기 위한 메커니즘과 해당 변경사항을 감독기구에 보고하기 위한 메커니즘

(l) 특히 (j)에서 언급한 조치의 검증 결과를 감독기구에 보고함으로써 확보할 수 있는, 사업체 집단 구성원의 규칙의 준수를 보장하기 위한 감독기구와의 협력 메커니즘

(m) 공동 경제활동에 종사하는 사업체 집단이나 기업 집단의 구성원이 제3국에서 적용을 받고, 의무적 기업 규칙이 보장하는 바에 실질적인 악영향을 미칠 가능성이 있는 법적 요건을 관할 감독기구에 보고하는 메커니즘

(n) 상시적 또는 정기적으로 개인정보를 열람(access)할 수 있는 인력을 대상으로 한 적절한 정보보호 교육

※ 현재 BCRs의 등록된 기업은 다음 사이트에서 확인할 수 있습니다.
http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

▪ 승인된 행동강령 및 인증 제도를 통해서도 국외이전의 적절한 안전조치로 인정될 수 있습니다.

4.3 자사의 개인정보의 이전이 국외이전의 특정한 예외상황에 해당하는지 확인하십시오.

▪ 특정한 상황의 특례에 해당하는 경우 국외이전이 가능합니다. (법 제49조 제1항)

① 정보주체가 적정성 결정 및 적절한 보호조치가 없음으로 인해 정보주체에 발생할 수 있는 정보이전에 대한 위험을 고지 받은 후, 정보주체가 이전에 명시적으로 동의한 경우

② 정보주체와 컨트롤러간의 계약 이행을 위해 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위해 정보이전을 해야 하는 경우

③ 정보주체의 이익을 위해 컨트롤러와 기타의 개인이나 법인 간에 체결된 계약의 이행을 위해 정보이전을 해야 하는 경우

④ 중요한 공익상의 이유로 정보이전이 반드시 필요한 경우

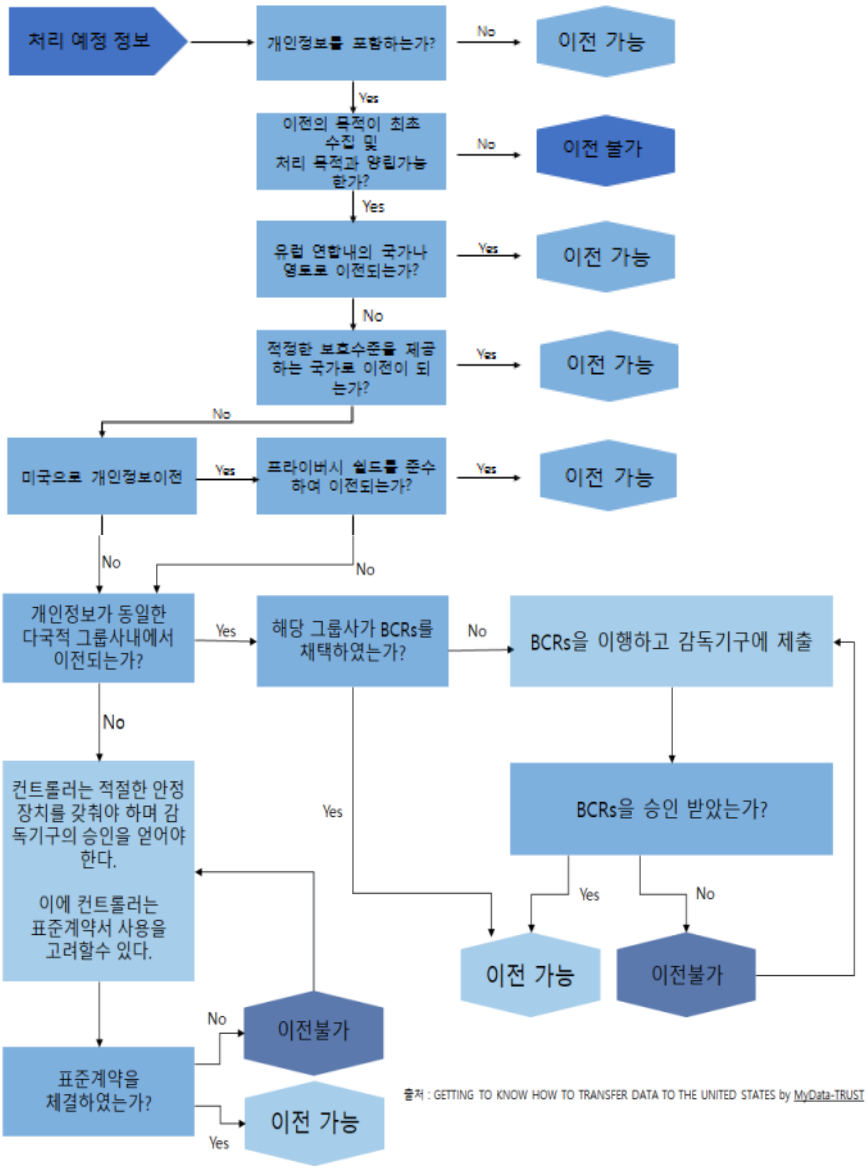
⑤ 법적 권리의 확립, 행사, 수호를 위해 정보이전이 필요한 경우

⑥ 정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우, 정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위해 정보이전이 필요한 경우

⑦ 개인정보가 EU 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 참조(조회)하기 위한 목적으로 만들어진 개인정보 기록부로부터 EU 또는 회원국 법률에 명시된 참조(조회)의 조건이 충족되는 범위 내에서 이전되는 경우

▪ 이러한 예외조항은 상당히 좁게 해석될 가능성이 높습니다. 따라서 대량의 개인정보를 구조적·지속적으로 전송하는 경우에 예외조항을 근거로 국외 이전을 하는 것은 바람직하지 않습니다. 다만, 일회적인 온라인 설문조사의 경우 예외조항의 적용 여부를 고려할 수 있습니다.

< 개인 정보 국외이전 체계>



출처 : GETTING TO KNOW HOW TO TRANSFER DATA TO THE UNITED STATES by MyData-TRUST

꼭 알아두기

- 외국에 위치한 정보를 제공받는 상대방이 누구든지 개인정보의 국외이전에 대한 규정이 적용될 수 있습니다.
- 표준조항의 경우 정보 이동의 변경에 따른 지속적인 업데이트가 필요할 수 있습니다.
- 다국적 기업의 경우 BCRs 채택을 고려해 볼 수 있습니다.
- 면제조항에 의존하는 것은 위험 관리에 적합하지 않습니다. 면제조항은 보통 좁게 해석된다는 점을 주의하시기 바랍니다.

관련 조문 및 근거

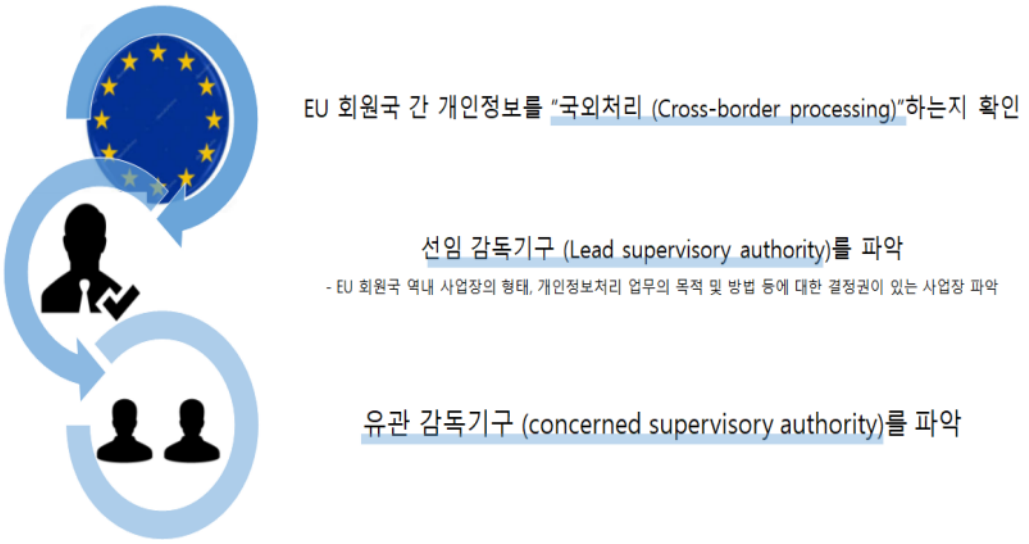
- 제44조(이전의 일반원칙)
- 제45조(적정성 결정에 근거한 이전)
- 제46조(적절한 보호조치에 따른 이전)
- 제47조(구속력 있는 기업규칙)
- 제48조(EU 법이 허가하지 않은 이전 또는 공개)
- 제49조(특정한 상황에 대한 특례)
- 전문 제110조

5. 선임 감독기구 파악 (Identifying a lead supervisory authority)

Check List

- EU 회원국 간 개인정보를 “국외처리(Cross-border processing)” 하는지 확인하시기 바랍니다.
- 선임 감독기구(lead supervisory authority)를 파악하시기 바랍니다.
  - EU 회원국 역내 사업장의 형태, 개인정보처리 업무의 목적 및 방법 등에 대한 결정권이 있는 사업장이 주사업장이고 사업장이 있는 국가의 감독기구가 선임 감독기구임
- 유관 감독기구(concerned supervisory authority)를 파악하시기 바랍니다.

< 선임 감독기구 파악(Identifying a lead supervisory authority) 절차 >



5.1 EU 회원국 간 개인정보를 “국외처리(Cross-border processing)” 하는지 확인하시기 바랍니다.

▪ 컨트롤러 또는 프로세서는 개인정보를 “EU 국가내로” 처리하는 경우에만 선임 감독기구를 파악하면 됩니다. 선임 감독기구는 기타 관련 감독기구 간 협력 조항에 규정된 절차에 따라 컨트롤러 또는 프로세서가 수행하는 회원국 간의 개인정보의 국외처리에 대한 법적 자격이 주어집니다.

▪ 개인정보의 “국외처리”는 다음 중에서 어느 하나에 해당하는 경우입니다.

① 컨트롤러 또는 프로세서가 하나 이상의 EU 회원국에서 개인정보를 처리하는 경우

② 컨트롤러 또는 프로세서가 EU 회원국 역내 단일 사업장을 운영하면서 개인정보를 처리하고 있으나, 해당 개인정보 처리로 인해 여러 EU 회원국의 정보주체에게 상당한 영향을 주거나, 또는 상당한 영향을 줄 가능성이 있는 경우

※ 정보주체에게 "1) 상당한 영향을 주거나 또는 2) 상당한 영향을 줄 가능성이 있는 경우"는 제29조 작업반이 발표한 "선임 감독기구의 식별에 관한 가이드라인(Guidelines for identifying a controller or processor's lead supervisory authority)"에서 다음의 경우에 해당한다고 설명하고 있습니다.

- 개인에 손해, 손실 또는 정신적 고통을 초래하는 경우
- 개인의 권리 및 기회를 제공받지 못하거나 제한받는 경우
- 개인의 건강, 복지 또는 심적 안정에 영향을 미치는 경우
- 개인의 재정 또는 경제적 상태 또는 상황에 영향을 미치는 경우
- 개인이 차별 또는 불공정한 처우를 방치하는 경우
- 민감정보 또는 불편한 정보 또는 특별히 아동 관련 정보의 분석이 포함된 경우
- 개인의 행동에 중대한 변화를 초래하는 경우
- 개인 관련 예상 밖의, 또는 예측 불가능하거나 원하지 않는 결과를 초래하는 경우
- 명예 훼손 등의 곤혹 또는 기타 부정적인 결과를 초래하는 경우
- "광범위"한 개인정보의 처리를 포함하는 경우

참 고

※ 원 스톱 숍 메커니즘(one-stop-shop mechanism)은 하나의 감독기구가 EU 회원국 시민들에 대한 개인정보의 국외처리에 대한 감독을 수행하도록 하는 개념입니다. 따라서 기업들은 어느 국가의 감독기구가 선임 감독기구가 될지 결정하여야 합니다. 다만 다음의 경우는 각 감독기구도 개인정보처리 관련 사건을 담당할 있는데, 이러한 경우는 원 스톱 숍 메커니즘에서 제외된다고 볼 수 있으니 참고하시기 바랍니다.

(i) 법령 위반에 관한 민원을 해결하거나 위반 가능성을 해결해야 하는 경우,
(ii) 관련 사항이 해당 회원국의 하나의 사업장만이 관련 있거나 해당 회원국의 정보주체에게만 중대한 영향을 미치는 경우

5.2 선임 감독기구(lead supervisory authority)를 파악하시기 바랍니다.

(1) 주 사업장(main establishment)을 식별하는 방법

1) 단일 사업장인 경우

▪ EU 역내 단일 사업장을 두고 있는 경우는 해당 사업장이 주 사업장이 되고, 해당 사업장이 위치하고 있는 국가의 감독기구가 선임 감독기구가 됩니다.

2) 하나의 컨트롤러가 있는 경우

▪ 컨트롤러가 EU 역내 여러 개의 사업장을 두고 있는 경우, 중앙관리지점(the controller's place of central administration)이 있다면 이 중앙관리지점이 주 사업장이 되고, 해당 사업장이 위치하고 있는 국가의 감독기구가 선임 감독기구가 됩니다.

▪ 위의 경우라고 하더라도 중앙관리지점이 아닌 다른 국가에 위치한 사업장이 "개인정보 처리에 대한 목적 및 방법 등의 결정"을 한다면, 해당 사업장이 주 사업장이 되고, 해당 사업장이 위치하고 있는 국가의 감독기구가 선임 감독기구가 됩니다. 이와 관련하여 가이드라인에서는 중앙관리지점이 아닌 다른 사업장이 주 사업장이 되는 조건을 다음과 같이 기술하고 있습니다.

① 개인정보 처리 업무에 대한 목적 및 방법 등을 어느 사정장에서 결정하는가?
② 개인정보 처리 업무 등을 포함한 비즈니스에 대하여 어느 사업장에서 결정하는가?
③ 결정사항이 효과적으로 구현하도록 하는 권한(power)을 가진 사업장은 어디인가?
④ 개인정보의 국외처리에 대한 전반적인 책임을 가진 DPO는 어느 사업장 소속인가?

3) 컨트롤러와 프로세서가 모두 있는 경우

▪ EU 역내 컨트롤러의 사업장이 있다면 해당 사업장이 주 사업장이 되고, 해당 사업장이 위치하고 있는 국가의 감독기구가 선임 감독기구가 됩니다. 이 경우 해당 선임 감독기구가 프로세서에 있어서도 선임 감독기구가 되고, 이 때 프로세서의 사업장이 위치한 국가의 감독기구가 유관 감독기구라고 볼 수 있습니다.

4) 프로세서만 있는 경우

▪ 프로세서만 있는 경우도 원 스톱 메커니즘의 적용을 받아서 컨트롤러가 있는 경우와 마찬가지로, EU 역내 중앙관리지점(the processor's place of central administration)이 있다면 이 중앙관리지점이 주 사업장이 되고 해당 사업장이 위치하고 있는 국가의 감독기구가 선임 감독기구가 됩니다.

5) 공동 컨트롤러의 경우

▪ GDPR은 공동 컨트롤러가 개인정보 국외처리를 하는 경우에 대해서 특별히 다루고 있지 않습니다. 이러한 경우 가이드라인에 따르면 공동 컨트롤러의 사업장 중에서 주 사업장을 결정해야 하고, 또한 선임 감독기구로 결정해야 한다고 설명하고 있습니다. 이 때 주 사업장을 결정하는 판단 조건은 2)에서 설명한 중앙관리지점이 아닌 다른 사업장을 주 사업장으로 결정하는 조건을 적용할 수 있습니다.

(2) 기타 주 사업장을 정하기 어려운 경우

▪ 위의 다양한 사업장의 행태 외에 여러 가지 복잡한 상황으로 주 사업장을 정하기 어렵거나 또는 개인정보 처리 업무를 어디에서 하는지 명확하게 결정하기 어려운 경우에도 GDPR에서는 여전히 선임 감독기구를 정하도록 하고 있습니다. 그럼에도 불구하고 선임 감독기구를 결정하기 어려운 경우는 이를 정하지 않을 수는 있으나, 이후 감독기구들이 어느 기관이 선임 감독기구로 적절할 지에 대해서 조사할 수 있습니다.

▪ 한편 기업이 하나의 회원국에 주 사업장을 두고 있기는 하나 관리활동 또는 개인정보처리에 대한 의사결정이 효과적/실제적으로 이행되고 있지 않은 경우, 관련 감독기구(또는 유럽 개인정보보호이사회)는 객관적 기준 및 증빙자료를 검토하여 어떤 감독기구가 선임 감독기구가 될 것인지 결정하게 됩니다.

5.3 유관 감독기구(concerned supervisory authority)를 파악하시기 바랍니다.

▪ 유관 감독기구는 다음 중 어느 하나의 사유로 개인정보 처리에 관여하는 감독기구를 의미합니다.

① 컨트롤러 또는 프로세서가 해당 감독기구가 소재한 EU 회원국의 영토에 설치된 경우
② 해당 감독기구가 소재한 EU 영토에 거주하는 정보주체가 개인정보 처리로 인하여 상당한 영향을 받거나 받을 가능성이 있는 경우
③ 민원이 해당 감독기구에 접수된 경우

참 고

▪ 사례1
- 네덜란드의 로테르담에 A 식품 소매업자의 본사(the place of central administration)가 있고, 다양한 EU 회원국들에 사업장이 있고 정보주체로부터 직접 개인정보를 수집하여 처리하고 있음
- 모든 사업장은 마케팅 목적을 위한 고객들의 개인정보를 처리하기 위해 동일한 소프트웨어를 사용하고 있음
- 마케팅 관련 고객정보 처리에 대한 목적 및 방법은 로테르담 본사가 결정하고 있음

☞ 위의 예제에서는 네덜란드 감독기구가 선임 감독기구가 됨

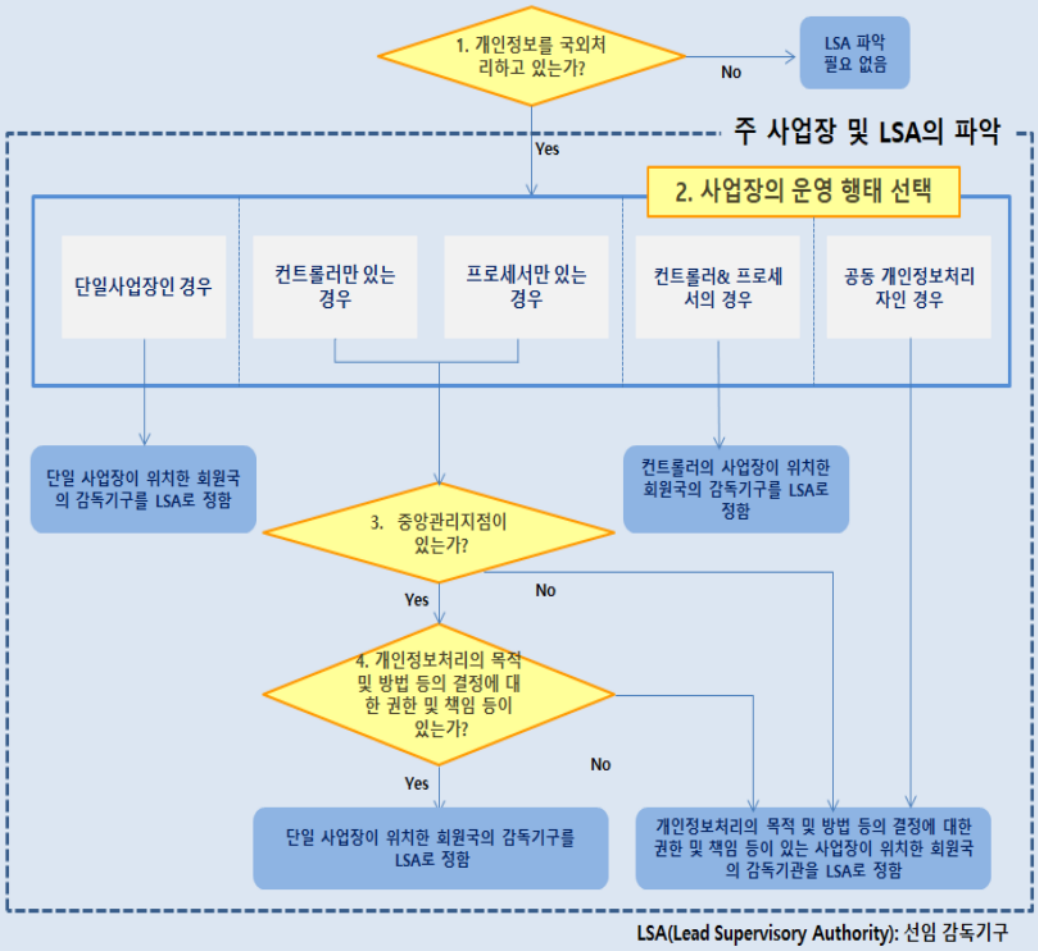
▪ 사례2
- A 은행은 독일 프랑크푸르트에 본사가 있고 모든 은행 업무는 본사에서 운영되고 있고 은행 관련 개인정보 처리는 독일에서만 이루어지고 있음
- 다만 보험업무 부서는 비엔나에 사업장이 있고, 이 사업장이 전체 EU 회원국 대상 모든 보험 업무에 대한 개인정보 처리업무 및 구현 등을 결정할 권한(power)이 있음

☞ 위의 예제에서는 오스트리아 감독기구가 선임 감독기구가 됨(보험업무 관련 개인정보의 국외처리)

☞ 독일 감독기구(Hessen supervisory)는 유관 감독기구로서 독일 로컬에서 수행되는 은행업무 관련 고객정보 및 HR 업무 등의 개인정보 처리를 관리함

꼭 알아두기

- 컨트롤러는 다음의 순서도를 따라서 어느 회원국의 감독기구가 자사의 선임 감독기구가 될지 판단하시기 바랍니다.



관련 조문 및 근거

- 제4조 21항(감독기구)
- 제4조 22항(유관 감독기구)
- 제4조 23항(회원국 간 정보처리)
- 제56조(선임 감독기구의 법적 자격)
- 제60조(선임 감독기구와 기타 유관 감독기구 간 협력)
- 전문 제36조
- 전문 제124 ~ 127조
- 전문 제131조

Ⅳ. 정보주체 권리 강화

1. 삭제권(잊힐 권리) (Right to erasure(right to be forgotten))

Check List

■ 삭제권(잊힐 권리)와 관련된 내부 지침 및 절차를 마련하십시오.

① 정보주체의 삭제권 보장 기준 및 절차

② 삭제를 거부할 수 있는 경우에 대한 기준 및 절차

③ 공개된 정보에 대한 삭제권을 보장하기 위한 절차

■ 처리되는 개인정보를 식별하고 흐름을 파악하십시오.

① 개인정보 식별

② 개인정보 흐름 분석

③ 개인정보 유형 별로 삭제 대상 및 기준을 식별하고, 삭제권을 거부할 수 있는 근거가 있는지 검토

■ 삭제권(잊힐 권리)을 보장하기 위한 체계를 수립하고 이행하십시오.

① 삭제 요구를 처리하는 창구 마련

② 삭제를 처리할 수 있는 관리적 또는 기술적 방안 적용

③ (필요 시) 개인정보를 제공받은 업체에게 해당 개인정보의 삭제를 통지할 수 있도록 협약 체결 및 통지방안 마련

④ 삭제가 적절히 이루어지고 있는지 정기적인 검토 수행

< 삭제권(잊힐 권리) – Right to erasure / be forgotten >

삭제권(잊힐 권리)와 관련된 내부 지침 및 절차 마련

정보주체의 삭제권 보장 기준 및 절차

삭제를 거부할 수 있는 경우에 대한 기준 및 절차

공개된 정보에 대한 삭제권을 보장하기 위한 절차

처리되는 개인정보를 식별하고 흐름 파악

개인정보 식별

개인정보 흐름 분석

개인정보 유형 별로 삭제 대상 및 기준을 식별하고, 삭제권을 거부할 수 있는 근거가 있는지 검토

삭제권(잊힐 권리)을 보장하기 위한 체계를 수립하고 이행

삭제 요구를 처리하는 창구 마련

삭제를 처리할 수 있는 관리적 또는 기술적 방안 적용

(필요시) 개인정보 제공받은 업체에게 해당 개인정보의 삭제를 통지할 수 있도록 협약 체결 및 통지방안 마련

삭제가 적절히 이루어지고 있는지 정기적인 검토 수행

1.1 삭제권(잊힐 권리)과 관련된 내부 지침 및 절차를 마련하십시오.

▪ 정보주체는 본인과 관련된 개인정보를 삭제하도록 요구할 수 있는 권리(삭제권)를 가집니다. 이에 따라 컨트롤러는 다음 중 하나에 해당하는 경우에는 부당한 지체 없이 해당 개인정보를 삭제하여야 합니다.(법 제17조 제1항)

① 개인정보가 수집 또는 처리 목적과 관련하여 더 이상 필요하지 않은 경우
② 정보주체가 개인정보 처리에 대한 동의를 철회하였으며, 해당 개인정보를 처리할 법적 근거가 없는 경우
③ 정보주체가 법 제21조(반대권) 제1항에 따라 개인정보의 처리에 반대하고, 관련 개인정보처리에 우선하는 정당한 사유가 없는 경우 또는 법 제21조 제2항에 의한 직접 마케팅(Direct marketing)에 정보주체가 반대하는 경우
④ 개인정보가 불법적으로 처리된 경우
⑤ EU 또는 EU 회원국 법령의 준수를 위해 개인정보의 삭제가 필요한 경우
⑥ 아동을 대상으로 한 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우

※ GDPR은 직접 마케팅(프로파일링 포함)에 대해서는 정보주체에게 절대적인 반대권을 보장하고 있으므로, 정보주체가 이에 반대하는 경우에는 조건 없이 해당 처리를 중지하고 관련 개인정보를 삭제하여야 합니다.

※ 잊힐 권리는 특별히 아동이 개인정보 처리에 관한 리스크를 완전히 인지하지 못한 상황에서 동의를 제공한 이후에 인터넷 상에서 이러한 개인정보를 삭제하고 싶어 하는 경우와 관련이 있습니다. 해당 정보주체가 더 이상 아동이 아니더라도 해당 권리를 행사할 수 있도록 하여야 합니다.

▪ 다만, 컨트롤러는 다음 중 하나에 해당될 경우에는 삭제 요구를 거부할 수 있습니다.(법 제17조 제3항)

① 표현(expression) 및 정보(information)의 자유에 관한 권리 행사를 위한 경우
② EU 또는 EU 회원국의 법적 의무를 준수하거나, 공익상의 업무를 수행하기 위해 또는 컨트롤러에게 부여된 공적 권한을 행사하기 위한 경우
③ 공익을 위한 보건 목적을 위한 경우
④ 공익적 기록보존(archiving purposes) 및 과학 또는 역사연구, 통계 목적을

위한 경우
⑤ 법적 청구권의 입증이나 행사 또는 방어를 위한 것인 경우

▪ 컨트롤러가 개인정보를 공개하고 해당 개인정보를 삭제할 의무가 있는 경우, 가용한 기술과 시행 비용을 참작하여 정보주체가 해당 개인정보의 링크, 복사본 또는 복제본의 삭제를 요구하였다는 사실을 다른 컨트롤러에게 알릴 수 있도록 기술적 조치 등 합리적 조치를 취해야 합니다.(법 제17조 제2항)

▪ 컨트롤러의 입장에서 정보주체의 삭제 요구에 적절히 대응하기 위해서는 사전에 아래의 내용을 포함한 내부 지침 및 절차를 마련할 필요가 있습니다.

- 정보주체의 삭제권을 보장하기 위한 기준 및 절차
- 삭제를 거부할 수 있는 기준 및 이에 따른 절차
- 공개된 정보에 대한 삭제 요구 절차 등

1.2 처리되는 개인정보를 식별하고 흐름을 파악하십시오.

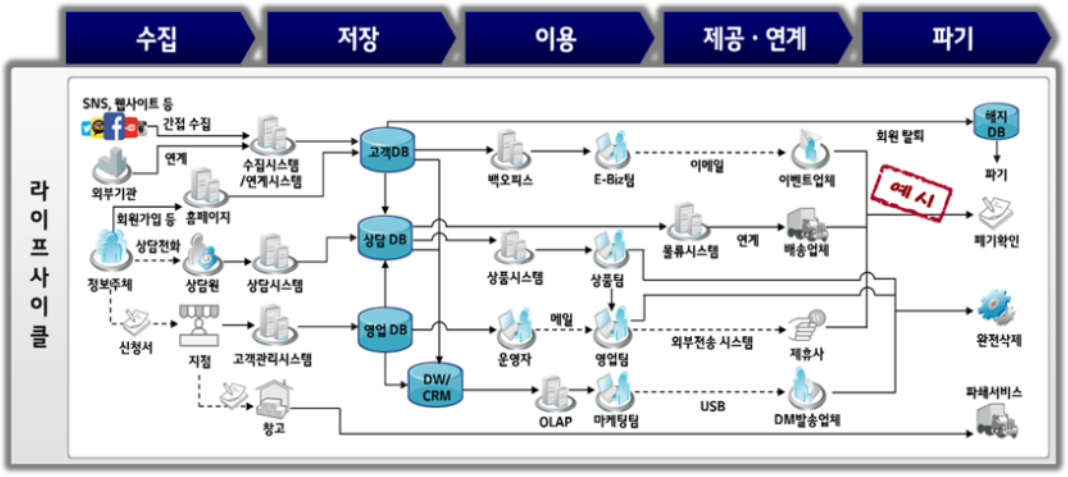
▪ 정보주체의 삭제 요구 등에 따라 관련된 개인정보를 빠짐없이 삭제하기 위해서는 우선적으로 삭제 대상이 되는 개인정보를 식별할 필요가 있습니다.

참 고

■ 수집 경로에 따른 개인정보의 유형(예시)
① 정보주체로부터 직접 수집한 개인정보
– 인터넷 홈페이지, 모바일앱 등 온라인을 통해 수집한 개인정보
– 대리점, 매장 등 오프라인을 통해 수집한 개인정보
– 전화 상담, 이메일 상담 등 고객센터를 통해 수집한 개인정보 등
② 서비스 이용과정에서 자동으로 수집되거나 생성된 개인정보
– 로그인 기록, 서비스 이용기록, 구매이력
– 프로파일링 등 사업자에 의해 생성된 정보 등
③ 다른 사업자 등을 통해 간접 수집한 개인정보
– 업무 제휴 등을 통해 다른 사업자로부터 제공받은 개인정보
– 인터넷 홈페이지 등 공개된 출처로부터 수집한 개인정보 등

▪ 다음으로는 해당 개인정보가 어디에서 어떻게 수집, 저장, 이용, 제공, 파기되는지 생명주기를 파악하고 흐름을 분석할 필요가 있습니다. 이때 흐름분석을 위해 특별히 정해진 방법이 존재하지는 않으며 개인정보의 유형, 서비스, 업무별로 주요한 개인정보 흐름이 쉽게 파악될 수 있도록 개인정보 흐름도를 작성하여 관리하는 방법이 일반적으로 활용되고 있습니다.

※ 개인정보 흐름도(예시)



▪ 이러한 개인정보 흐름분석을 바탕으로 컨트롤러는 정보주체로부터의 삭제요구에 대하여 원천 개인정보와 그로부터 복제되거나 파생된 정보를 추적함으로써 삭제가 필요한 정보를 빠짐없이 식별하고 신속하게 삭제할 수 있습니다. 또한, 제공·연계된 개인정보와 수령인을 식별함으로써 필요 시 해당 수령인에게 개인정보 삭제에 관한 사항을 통지할 수 있습니다.

1.3 삭제권(잊힐 권리)을 보장하기 위한 체계를 수립하고 이행하십시오.

▪ 앞서 수립된 내부 지침 및 절차와 개인정보 흐름분석 결과를 바탕으로 삭제권(잊힐 권리)을 보장하기 위한 체계를 수립하고 이행하여야 합니다.

① 정보주체의 삭제요구를 접수하고 처리하는 창구 마련

- 정보주체가 쉽게 삭제요구를 할 수 있도록 인터넷, 이메일, 전화 등 다양한 접수 방법 제공

- 정보주체의 삭제 요구를 처리할 담당 조직을 지정하고 책임 및 역할 정의

② 삭제를 처리할 수 있는 관리적 또는 기술적 방안 적용

- 삭제 요구를 거부할 수 있는 경우인지 판단할 수 있는 기준 및 절차를 마련하고 이행

- 흐름 분석 결과를 반영하여 복제본, 사본 등도 빠짐없이 삭제될 수 있도록 조치

③ (개인정보를 외부에 공개 또는 제공한 경우) 개인정보를 제공받은 업체에게 해당 개인정보의 삭제를 통지할 수 있도록 협약 체결 및 통지방안 마련 (법 제17조 제2항)

- 흐름분석 결과를 바탕으로 외부 공개 및 제공 흐름 식별

- 개인정보를 제공받은 업체와 삭제권 보장을 위한 협약 체결(통지 방법, 통지를 받았을 때 조치 사항, 책임 소재 등)

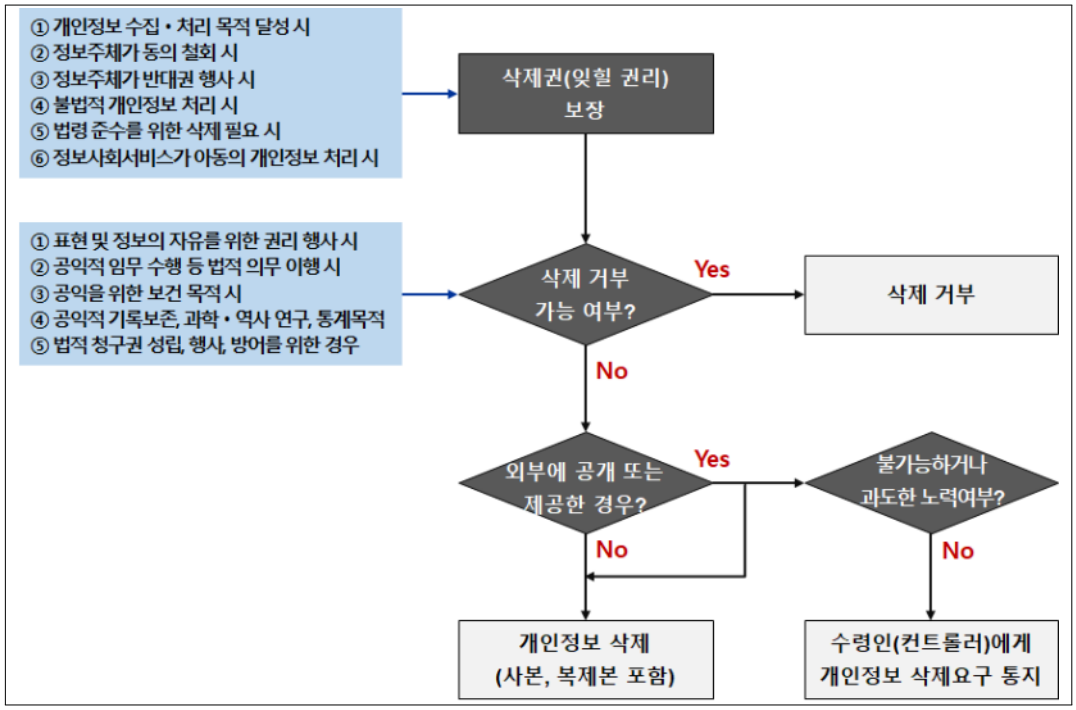
- 해당 업체와 체결된 협약에 따른 삭제 요구 통지방법 이행

④ 개인정보 삭제가 적절히 이루어지고 있는지 정기적인 검토 수행

- 제3자 제공업체 추가 등 개인정보 흐름상의 변화가 있는지 정기적으로 확인하여 변화가 있는 경우 관련 사항 반영

- 개인정보의 삭제가 적절이 수행되고 있는지 분기, 반기 등 기간을 정하여 정기적으로 검토 및 개선

※ 개인정보 삭제권(잊힐 권리) 처리 절차



꼭 알아두기

- 개인정보 처리 업무별로 처리의 근거, 목적을 파악하여 개인정보의 삭제가 필요한 경우와 삭제를 거부할 수 있는 경우를 명확히 정의하여야 합니다.
- 개인정보 흐름분석을 통해 삭제 대상이 되는 모든 개인정보의 저장 위치, 형태, 담당부서 등을 파악하여 복제본, 백업본, 사본 등도 빠짐없이 삭제될 수 있도록 하여야 합니다.
- 만약 개인정보를 수령인에게 제공 또는 공개하였다면 해당 개인정보의 링크, 사본, 재현물이 삭제될 수 있도록 요청사항 통지 등 합리적인 조치를 취해야 합니다.

관련 조문 및 근거

- 제17조(삭제권('잊힐 권리'))
- 제19조(개인정보의 수정이나 삭제 또는 처리의 제한에 관한 고지의무)
- 전문 제65~66조

2. 개인정보 이동권(Right to data portability)

Check List

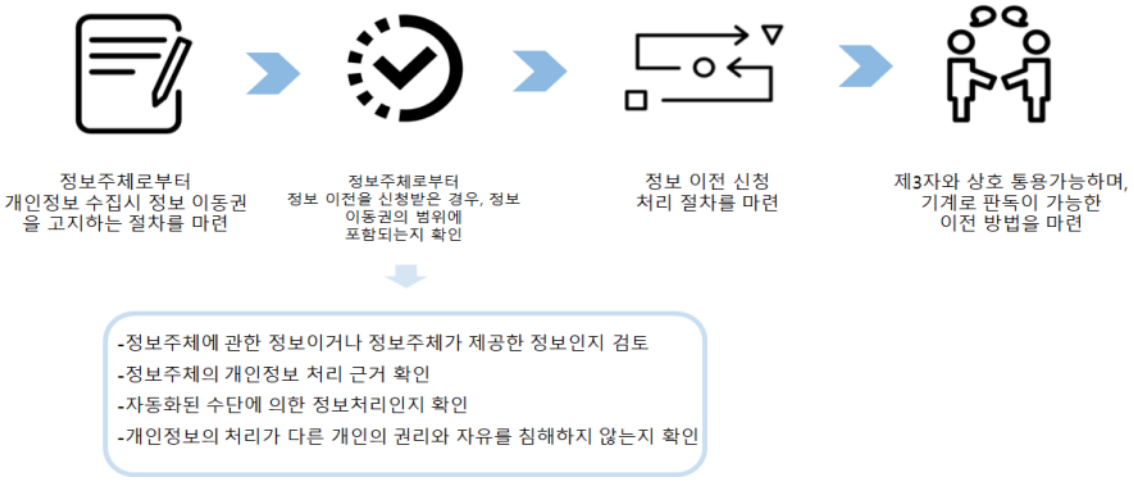
- 정보주체로부터 개인정보 수집 시 개인정보 이동권을 고지하는 절차를 마련하십시오.
- 정보주체로부터 정보 이전을 신청 받은 경우, 개인정보 이동권의 범위에 포함되는지 확인하십시오.

① 정보주체에 관한 개인정보이고 정보주체가 제공한 정보인지 검토
② 정보주체의 개인정보 처리 근거 확인
③ 자동화된 수단에 의한 정보처리인지 확인
④ 개인정보의 처리가 다른 개인의 권리와 자유를 침해하지 않는지 확인

- 정보 이전 신청 처리 절차를 마련하십시오.
- 제3자와 상호 통용가능하며, 기계로 판독이 가능한 이전 방법을 마련하십시오.

개인정보 이동권은 GDPR에 신설된 정보주체의 새로운 권리입니다. 이 권리는 1) 정보주체가 컨트롤러에게 제공한 개인정보를 본인이 받을 수 있도록 하고, 2) 또한 정보주체의 개인정보를 다른 컨트롤러에게 이전이 가능하도록 해 줍니다. 이 때 컨트롤러는 개인정보를 체계적으로 구성되고 일반적으로 통용되며 기계판독이 가능한 형태로 제공해야 합니다. 이 새로운 권리의 목적은 정보주체에게 본인의 정보와 관련된 권한을 부여하기 위한 것이고, 또한 정보주체와 컨트롤러 간의 관계가 재균형(re-balance)을 이룰 수 있도록 기회를 제공하는 것입니다.

< 개인정보 이동권(Right to data portability) >



2.1 정보주체로부터 개인정보 수집 시 개인정보 이동권을 고지하는 절차를 마련하십시오.

▪ 컨트롤러는 정보주체에게 개인정보 이동권에 대하여 알려야 합니다.

① 개인정보를 정보주체로부터 직접 수집한 경우에는 개인정보를 입수한 시점에 반드시 행해져야 함

② 개인정보를 정보주체로부터 직접 수집하지 않은 경우에는 해당 데이터 수집 시점부터 1개월 이내에 알려야 함

※ 개인정보를 정보주체에게 연락할 목적으로 이용하는 경우에는 최초 연락 시점에 알려야 하며, 제3자 제공을 하는 경우에는 최초로 제3자에게 제공되는 시점에 알려야 함

▪ 컨트롤러는 개인정보 이동권과 다른 권리를 구별할 수 있도록 명확하고 포괄적인 정보를 제공해야 합니다. 아울러 컨트롤러가 정보주체에게 열람권과 개인정보 이동권을 통해 받을 수 있는 정보의 종류에 차이가 있다는 점을 명확하게 설명해야 합니다.

※ 삭제권(제17조)과의 관계

- 정보주체가 개인정보 삭제권을 행사하는 경우, 컨트롤러는 개인정보 이동권을 이유로 개인정보의 삭제를 연기하거나 거부할 수 없습니다.

※ 보관기간 관련

- 단순히 미래에 발생할 지도 모르는 정보이전요청에 응하기 위해 필요 이상으로 개인정보를 보관하거나 구체적으로 정해진 보관기간을 초과하여 개인정보를 보관할 의무가 없으며, 전송되는 개인정보에 적용되는 정보의 보관기간에도 영향을 미치지 않습니다.

2.2 정보주체로부터 정보 이전을 신청받은 경우, 개인정보 이동권의 범위에 포함되는지 확인하십시오.

▪ 개인정보 이동권의 범위에 해당하는 정보는 아래와 같습니다.

① 정보주체와 관련된 개인정보(예: 핸드폰, 채팅/메시지 정보, 인터넷 상의 기록 등)

② 정보주체가 컨트롤러에게 제공한 개인정보(예: 이름, 주소, 나이 등)

※ 개인정보 이동권의 범위에는 익명 정보(anonymous data)나 정보주체와 관련되지 않는 정보는 해당하지 않습니다. 다만 가명정보(pseudonymous data)는 특정 개인에 연결시킬 수 있는 정보이므로 개인정보 이동권의 범위에 포함됩니다.

※ 개인정보 이동권 행사 시, 컨트롤러에 의해 추론되거나 파생된 정보(inferred data and derived data)는 이동권 행사의 대상이 되지 않습니다.

▪ 개인정보 이동권은 개인정보처리 근거가 1) 정보주체의 동의가 있거나, 또는 2) 정보주체가 계약당사자인 계약(고용 계약 포함)을 이행하기 위하여 개인정보 처리를 하는 경우 3) 처리가 자동화된 수단에 의해서 이행되는 경우에만 인정됩니다. (제20조 제1항)

※ 개인정보의 처리 근거가 컨트롤러나 제3자의 정당한 이익의 실현을 위한 경우에는 개인정보 이동권이 인정되지 않고, 법적의무를 준수하기 위하여 또는 공적인 업무 수행을 위하여 개인정보를 처리는 경우에도 개인정보 이동권은 인정되지 않습니다.

▪ 개인정보 이동권의 범위에 포함되는 개인정보는 자동화된 수단에 의해 처리되는 정보입니다. 그러므로 종이 문서들은 범위에 해당되지 않습니다.

▪ 개인정보 이동권으로 제공되는 개인정보는 다른 정보주체의 권리 및 자유에 불리한 영향을 주지 않는 정보이어야 합니다.

▪ 아래의 개인정보 이동권의 범위 관련 체크리스트에 모두 해당하는 경우

개인정보 이동권의 범위에 포함됩니다.

① 정보주체에 관한 정보 또는 정보주체가 제공한 개인정보인지?
② 개인정보 처리에 대한 법적 근거가 정보주체의 동의 또는 계약의 이행을 위한 목적인지?
③ 개인정보가 자동화된 방식으로 처리되는지?
④ 제공하는 개인정보가 다른 정보주체의 권리 및 자유에 불리한 영향을 미치지 않는지?

2.3 정보 이전 신청 처리 절차를 마련하십시오.

▪ 정보 이동의 신청 처리절차는 다음과 같습니다.

① 정보주체의 신청 접수
② 담당부서에서 적법한 정보 이동 신청인지를 검토
③ 정보주체의 신청을 처리할 수 없는 경우 접수일로부터 1개월 이내에 조치를 취하지 않은 사유와 함께 감독기구에 민원을 제기하거나 소송을 제기할 수 있다는 사실을 정보주체에게 통지
④ 정보주체의 신청을 처리할 수 있는 경우 신청일로부터 1개월 이내로 정보 이동 처리 후 신청인에게 통지
⑤ 신청의 내용이 복잡하거나 여러 건의 신청이 있어 1개월 이상의 시간이 소요될 경우 접수일로부터 1개월 이내에 연장 사유와 연장 기간(2개월까지)을 신청인에게 고지

▪ 컨트롤러는 정보주체가 자신의 개인정보에 대한 개인정보 이동권을 쉽게 행사할 수 있는 양식(modalities)을 제공하여야 하고, 컨트롤러가 전자적 수단으로 개인정보를 처리하는 경우에는 정보주체가 전자적 방식으로 권리를 행사할 수 있는 수단도 함께 제공하여야 합니다.

▪ 컨트롤러는 신청자의 신원을 확인하여 정보 이동을 신청할 권리가 있는 정보주체인지 여부를 확인하여야 합니다.

▪ 컨트롤러는 부당한 지체 없이(without undue delay) 정보주체에게 제공하여야 하며, 정보 이동 신청 접수 후 1개월 이내로 컨트롤러가 취한 정보

이동 관련 정보를 제공하여야 합니다. 이동 신청한 정보처리가 복잡하여 시간이 소요될 경우 1개월 이내에 연장 사유와 연장 기간(2개월 연장 가능, 총 소요기간 최장 3개월)에 대하여 고지하여야 합니다.

- 만약 컨트롤러가 정보주체의 신청에 대하여 아무런 조치를 취하지 않을 경우, 컨트롤러는 지체 없이 신청일로부터 1개월 이내에 조치를 취하지 않은 사유와 감독기구에 사법 구제를 요청할 수 있음을 정보주체에게 고지하여야 합니다.

- 정보의 이동은 무료로 제공되어야 합니다. 정보 이동의 신청 근거가 없거나 과다하다고 입증할 수 있는 경우를 제외하고는 컨트롤러가 개인정보 이동에 대한 비용을 청구하는 것을 금지하고 있습니다. 신청의 과다함 여부를 판단할 때는 신청 건별로 판단하여야 하고, 단일의 정보주체가 신청한 총 신청 건수를 합산할 수 없습니다. 이러한 점에서, 정보 이동 시스템 운영비용을 정보주체에게 청구할 수 없으며, 비용이 소요된다는 이유로 개인정보 이동권 권리 행사를 거절할 수 없습니다.

2.4 제3자와 상호 통용가능하며, 기계로 판독이 가능한 개인정보 이전 방법을 마련하십시오.

- 정보주체는 컨트롤러에게 제공한 개인정보를 본인이 수령할 수도 있고, 기술적으로 가능한 경우에는 다른 컨트롤러로 직접 제공하도록 신청할 수도 있습니다.

- 컨트롤러는 정보주체로부터 정보 이동 신청을 받은 경우에 개인정보를 “체계적으로 구성되고 일반적으로 널리 이용되며 기계에 의해 판독이 가능한 형식(a structured, commonly used and machine-readable format)”으로 제공해야 합니다. 그 이유는 개인정보 이동권이 열람권과 달리 정보주체와 컨트롤러 간 관계의 재균형(re-balance)을 위해서 “재사용(reuse)”이 가능한 형식으로 제공해야 하기 때문입니다.

※ 참고로 업계나 서비스 등에서 정해진 형식이 있지는 않지만, 주로 재사용(reuse)이 가능한 메타데이터이면서 개방형 형식인 CSV, JSON, XML 등으로 개인정보가 제공될 것입니다.

▪ 또한 GDPR은 컨트롤러가 상호운용이 가능한 형식(interoperability of the data format)으로 개인정보를 제공하도록 독려하고 있습니다. 하지만 반드시 다른 컨트롤러와 개인정보를 주고받을 수 있도록 기술적으로 호환 가능한(technically compatible) 처리시스템을 채택 또는 유지할 의무가 발생하지는 않습니다.

▪ 컨트롤러는 기술적 차원에서 정보주체 또는 다른 컨트롤러에게 개인정보를 제공하기 위한 경로에 대하여 아래와 같은 방법을 고려해야 합니다.

① 데이터의 전체 데이터세트(또는 글로벌 데이터세트의 일부 추출 데이터)를 직접 전송

② 관련 데이터 추출을 가능하게 하는 자동화 수단

※ 컨트롤러가 다른 컨트롤러 또는 프로세서에게 정보를 제공하는 방법으로 응용 프로그래밍 인터페이스(Application Programming Interface, API)를 제공하는 방안을 고려할 수 있습니다.

▪ 컨트롤러는 개인정보 이동시 정보의 손실, 파괴, 손상으로부터 보호하기 위하여 적절한 기술적·관리적 조치를 통해 개인정보의 보안 상태를 유지하여야 하며, 컨트롤러에게 남아있는 정보를 계속해서 안전하게 보관하여야 합니다.

▪ 개인정보를 공동으로 처리하는 공동 컨트롤러의 경우, 계약을 통해 데이터 이동의 요청 처리에 관한 각 컨트롤러의 책임을 명확히 배분할 필요가 있습니다.

참 고

▪ 사례1 : 영국의 Midata

- 영국에서 정부주도로 2011년부터 시작되었으며 소비자 권리 보호를 위해 일부 민간기업을 대상으로 최근 12개월간의 개인 거래내역을 'midata' 파일 형식으로 내려 받을 수 있도록 한 제도입니다. 정보주체는 제공받은 Midata를 이용해서 가격비교 사이트(Comparison Provider)에

제출하여 소비자는 맞춤형 정보를 얻을 수 있습니다. 아래 표는 midata에서 제공하는 데이터의 예시를 보여주고 있습니다.

Draft midata minimum standard (예시)				
Date	**Type**	**Merchant/ Description**	**Debit/Credit**	**Balance**
04/03/2014	VIS	Boots the Chemist	£5.00	£260.00
04/03/2014	DD	Fitness First	-£50.00	£255.00
03/03/2014	ATM	ATM withdrawal	-£100.00	£305.00
03/03/2014	TRF	etc.	-£20.00	£405.00
02/03/2014	VIS	etc.	-£75.00	£425.00
01/03/2014	CSH	etc.	-£50.00	£500.00

▪ 사례2 : 프랑스의 MesInfos의 SelfData

- MesInfos는 프랑스에서 2500~3000여명의 소비자(개인), 에너지, 보험, 은행, 통신 등의 8개 업체를 연결하는 플랫폼을 제공하는 프로젝트로서, 현재 파일럿 단계를 진행 중입니다.
- SelfData의 역할은 개인에게는 자신의 정보통제가 가능하도록 하는 것이고, 기업에게는 데이터의 품질을 향상시키는 기회를 주는 것입니다. 제공하는 정보의 범위는 소비데이터(영수증, 인보이스 등), 금융, 에너지, 통신, 웹 브라우징, 건강, 교육, 고용 및 행정정보 등입니다. SelfData에서 제공하는 서비스는 아래와 같습니다.

① 개인이 기업에게서 기업의 정보 시스템에 있는 자신의 개인정보(수집되거나 시스템에서 생성된 개인정보)를 제공받을 수 있음

② 제공받은 개인정보를 개인용 클라우드와 같은 개인정보 관리시스템에 보관 및 관리가 가능함

③ 개인적 또는 비즈니스적인 목적으로 더 나은 의사결정을 위하여 제3자의 응용 프로그램 및 서비스를 이용 가능함

▪ 사례 3 : 기업의 구현 사례

- 구글(Google)은 CSV, JSON, vCard 등과 같이 재사용이 가능한 형식으로 정보주체에게 개인정보를 제공하고, 실제 다운로드 신청절차 및 방법은 아래 URL에서 확인이 가능함

  https://support.google.com/accounts/answer/3024190?hl=ko

꼭 알아두기

- 개인정보 이동권은 다른 개인의 권리와 자유를 침해하지 않아야 하므로, 정보주체의 개인정보 이동권의 행사가 다른 개인의 권리와 자유(영업비밀, 지식재산권 등)를 침해하는 경우 정보의 이동이 제한될 수 있습니다.
- 정보주체가 제3자에게 정보를 이전해 줄 것을 요청하여 제3자가 정보를 이전받은 경우, 제3자는 이전 받은 개인정보에 관하여 새로운 컨트롤러가 되므로, 정보주체는 새 컨트롤러의 개인정보 처리에 대하여 동의하거나 개인정보 처리에 관한 계약을 체결하여야 하고, 새 컨트롤러는 GDPR 제5조의 개인정보 처리 원칙을 준수하여야 합니다.
- 정보주체가 개인정보 이동권을 행사한 후에도 컨트롤러는 정보주체의 개인정보를 처리하는 한 계속 컨트롤러의 지위를 유지합니다.

관련 조문 및 근거

- 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식)
- 제13조(정보주체로부터 개인정보를 수집하는 경우, 제공되는 정보)
- 제17조(삭제권)
- 제20조(개인정보 이동권)
- 전문 제59조
- 전문 제68조
- 전문 제73조
- 전문 제156조

3. 자동화된 결정 및 프로파일링 관련 권리

Check List

- 조직 내 프로파일링 현황을 파악하고 프로파일링의 요건을 확인하십시오.
  - ① 프로파일링을 위한 정보 처리가 자동화된 형태로 이루어집니까?
  - ② 정보처리의 목적이 개인의 특성 평가를 하기 위함입니까?
  - ③ 프로파일링이 개인정보에 기반하여 이루어집니까?
- 프로파일링을 기반으로 자동화된 의사결정이 이루어지는지 확인하십시오.
- 자동화된 의사결정이 유발하는 효과를 확인하십시오.
  - ① 정보주체 대상 법적 효과가 있습니까?
  - ② 법적 효과와 유사한 중요한 효과가 있습니까?
- 자동화된 의사결정을 활용하는 업무의 수행 근거를 확인하십시오.
  - ① 컨트롤러와 정보주체의 계약 이행을 위해 필요합니까?
  - ② 법적 근거가 있습니까?
  - ③ 정보주체의 동의를 받았습니까?
- 정보주체의 권리 보장 절차를 마련하십시오.
- 민감정보와 아동의 개인정보가 처리되는지 확인하십시오.
- 보호조치(safeguard)를 수립하십시오.
- 자동화된 의사 결정을 개인정보 영향평가(DPIA) 대상에 포함하십시오.
- 프로파일링에 GDPR 개인정보보호 원칙의 적용 여부를 확인하십시오.

< 자동화된 결정 및 프로파일링 관련 권리 >

3.1 조직 내 프로파일링 현황을 파악하고 프로파일링이 개인정보의 자동화 처리를 기반으로 개인의 특성 평가를 위해 이루어지는지 확인하십시오.

▪ 프로파일링 행위와 유형은 매우 다양하며 마케팅 및 맞춤형 서비스 제공 뿐 아니라 수사 및 치안 등 공공과 민간을 아우르며 널리 활용되고 있습니다. 따라서 조직 내에 정보주체를 프로파일링 하는 개인정보 처리 현황을 파악해야 합니다. 또한, 파악된 프로파일링 절차가 GDPR 상에서 규정하는 프로파일링의 개념에 해당하는지를 확인할 필요가 있습니다.

▪ GDPR에서 프로파일링이란 개인(또는 개인이 속한 집단)에 대한 자동화 처리되는 개인정보를 기반으로 개인의 특성 또는 행동패턴을 분석하여 특정 범주 또는 그룹에 배치하고 현재 또는 미래의 행동 특성을 추론하는 행위를 말합니다. 단순히 연령, 성별, 키 등과 같은 특징에 기반하여 개인을 구분하고 평가하는 행위 또한 동 프로파일링의 개념에 포함됩니다.

▪ GDPR의 규제 대상 프로파일링은 다음의 3가지 요건을 모두 충족해야 합니다.

① [처리 방식] 프로파일링이 자동화된(automated) 정보 처리에 의해 이루어지는 경우

- 이는 프로파일링 과정이 오로지 자동화된 정보처리에 의해서만 이루어져야 한다는 것을 의미하는 것은 아닙니다. 일부 인적 개입(human intervention)이 있다고 하더라도 GDPR상 프로파일링의 개념에 해당될 수 있습니다.

② [목적성] 정보처리의 목적이 개인의 특성을 평가하기 위함인 경우

- 개인의 특성이란 개인의 근무 성과, 경제적 상황, 건강, 개인적 선호, 관심, 신뢰성, 행태, 위치나 움직임 등이 해당됩니다. 정보 처리의 목적이 이와 같은 개인의 특성 평가가 아니라면 GDPR 상의 프로파일링에 해당되지 않습니다.

※ 온라인 서비스에 봇(bot)이 무분별하게 대량으로 로그인 하는 것을 방지하기 위해 일정한 질문을 제시하고 답변을 입력받아 이를 분석한 후에 로그인 절차를 진행하는 경우, '자동화된' 개인정보의 처리가 발생하나, 이는 봇(bot)과 사람을 구별하려는 판단 목적만 존재하기 때문에 프로파일링이라 할 수 없습니다.

③ [처리 대상] 프로파일링이 개인정보에 기반하여 이루어지는 경우

참 고

■ 프로파일링의 정보 처리 3단계

단계	의미	예시
데이터 수집	개인 또는 그룹에 대한 정보 수집	데이터 브로커가 공공·민간 영역에서 고객 요청이나 내부적 목적으로 데이터 수집
상관성 확인을 위한 자동화된 분석	특성 또는 행동 패턴 분석	데이터 브로커가 데이터를 가공하여 개인에 대한 프로파일을 개발하고 세그멘트(Segment)에 배치
개인에게 상관관계를 적용하여 현재 또는 미래의 행동 특성을 식별	개인에 대한 예측 또는 평가 수행 - 업무 수행 능력 - 관심사 - 예측되는 행동	- 데이터 브로커가 상품 및 서비스의 타게팅 개선 계획 중인 기업 대상 데이터를 판매 - 개인 관심사에 따라 개인을 특정 카테고리에 배치하여 프로파일링 수행

※ 세그멘트(Segment) : 타겟 마케팅 및 맞춤형 서비스 제공 등 업무 목적을 위해 개인을 그룹으로 분류하는 최소 기준

3.2 프로파일링을 기반으로 자동화된 의사결정이 이루어지는지 확인하십시오.

▪ 정보주체는 프로파일링 기반 자동화된 의사 결정(automated decision making)의 대상이 되지 않을 권리를 가집니다. 따라서 프로파일링을 기반으로 자동화된 의사 결정이 이루어지는지를 확인해야 합니다.

▪ 자동화된 의사결정이란 다양한 데이터에 기반하여 인적 개입 없이 기술적 수단만으로 개인에 대해 중요한 의사 결정을 하는 것을 의미합니다.

※ 자동화된 의사결정을 위해 활용되는 다양한 데이터 수집의 예시

정보주체가 직접 제공한 데이터	설문지 응답 등
관찰된 데이터	앱을 통해 수집된 위치 정보 등
기수집된 개인 프로필 기반으로 생성되거나 추정된 데이터	신용 정보 등

▪ 자동화된 의사결정은 프로파일링을 기반으로 할 수도 있고, 프로파일링과 별도로 이루어질 수 있습니다. 또한 프로파일링을 기반으로 하더라도 자동화된 의사 결정 과정이 아닐 수도 있습니다. GDPR에서는 1) 프로파일링에 기반하여 2) 의사 결정이 자동으로 이루어지는 경우만을 규제를 합니다.

※ 프로파일링과 자동화된 의사 결정의 유형(두 번째 유형만 해당)

사례	프로파일링 여부	자동화된 의사 결정 여부
과속카메라에서 차량 속도를 확인하여 과속 위반 벌금을 부과	X	O
과속 운전의 반복성 여부 혹은 다른 교통 법규 위반 여부 등 운전자의 평소 운전 습관을 모니터링 및 평가하여 자동으로 벌금액을 결정	O	O
은행 담당자가 대출 신청자의 신용 등급을 고려하여 대출 여부를 결정	O	X

▪ 특히 GDPR에서 규제하는 자동화된 의사 결정은 그 과정이 완전 자동화(solely automated)되어야 합니다.

- 완전 자동화된 의사 결정이란 프로파일링을 기반으로 한 의사 결정 과정에서 인적 개입(Human Intervention)이 전혀 없는 것을 의미합니다. 프로파일링을 기반으로 정보주체에게 영향을 미치는 분석 결과가 도출되었을 때 사람이 이를 리뷰하고 다른 요소를 고려하여 최종 결정을 한다면 이는 완전 자동화된 의사 결정으로 보기 어렵습니다.

참 고

■ 프로파일링 활용 유형

① 일반적 프로파일링

② 프로파일링에 기반한 의사 결정 : 자동화되어 작성된 프로파일을 기반으로 은행 담당자가 검토(인적개입)하여 대출 여부 결정

③ 프로파일링에 기반한 완전 자동화된 의사 결정(solely automated decision making) : 대출 여부를 알고리즘이 결정하고 사람의 유의미한 검토 없이 그 결과가 자동으로 개인에게 통보

▪ 다만, 의사 결정 과정에 일부 인적 개입이 있더라도 이것이 결과에 실질적인 영향을 미치지 않는다면 유효한 인적 개입으로 보기 어렵습니다. GDPR에서 의미하는 인적 개입이란, 사람이 개입하여 수행하는 자동화된 의사 결정에 대한 검토가 형식적이지 않고 유의미해야 합니다. 유효하지 않는 인적 개입이 의사 결정 과정 단계에 포함되더라도 동 의사 결정은 완전 자동화 의사 결정의 범주에서 벗어날 수 없습니다.

※ 유효한 인적 개입의 요건

① 충분한 권한과 책임이 되는 사람에 의해 수행되어 자동화된 의사 결정의 변경이 가능해야 함

② 검토를 위해 사용 가능한 모든 입출력 정보(프로파일링에 활용된 정보, 알고리즘에 의해 도출된 정보)를 활용해야 함

3.3 자동화된 의사결정이 유발하는 효과를 확인하십시오.

▪ 정보주체는 자동화된 의사 결정의 대상이 되지 않을 권리가 있습니다. 단, 동 의사 결정이 정보주체에게 1) 법적 효과(legal effect)가 있거나 2) 법적 효과와 유사한 중요한 효과(similarly significant effect)가 있는 경우에만 해당이 됩니다. 따라서 프로파일링을 기반으로 하는 자동화된 의사 결정을 확인하였다면 동 의사 결정에 따른 효과 또한 확인해야 합니다.

▪ 법적 효과(legal effect)란 결사의 자유, 투표의 자유 등 정보주체의 법적

권리 혹은 법적 상태에 영향을 줄 수 있는 것을 의미합니다. 다시 말해, 개인의 법적 상태, 권리, 자유, 시민권 등에 변화를 발생시키는 경우나 은행, 보험, 채용 등의 계약 행위 등이 해당 됩니다.

☞ **(예시)**

① 양육 혹은 주택 지원제도 등 국가 사회 보장 제도의 부여 혹은 제한
② 국경 입국 거부
③ 관할 당국에 의한 강화된 보안 및 감시를 받는 경우
④ 통신 요금 미납으로 휴대폰 이용 정지

▪ 법적 효과와 유사한 중요한 효과(similarly significant effect)란 정보주체의 법적 권리에 영향을 미치지 않더라도 동등하거나 유사한 의미를 갖는 효과를 발생시키는 경우입니다. 비록 의사 결정의 결과가 법적 권리 또는 의무에 특별히 법적 영향을 주지 않더라도 정보주체는 보호를 요구하기에 충분할 만큼의 영향을 받을 수가 있기 때문입니다.

- 그 기준을 EU에서는 명확히 밝히고 있지 않으나, 개인의 상황, 행동, 선택에 중대한 영향을 줄 가능성이 있는 학교 입학, 세금 감면, 승진 및 보너스 지급 등이 이에 해당됩니다.

▪ 법적 효과나 유사한 중요 효과가 없더라도 컨트롤러는 프로파일링 기반 자동화된 의사 결정 행위에 대해서는 GDPR 제4장에서 규정하는 정보주체 권리보장을 위한 일반적 보호 조치를 취하여야 합니다.

참 고

[온라인 광고 적용 여부]

■ 프로파일링 기반 온라인 광고는 GDPR 상의 프로파일링 기반 자동화된 의사 결정에 해당 될 수도 있고 안 될 수도 있는데 온라인 광고가 가진 효과성을 기준으로 아래의 관점에서 판단해야 합니다.

① 프로파일링 프로세스의 개입 수준
② 정보주체가 고려하는 기대 수준과 희망 사항
③ 광고 전달 방식
④ 타겟이 되는 정보주체의 취약성

■ 이를테면 “서울에 거주하는 여성”과 같은 특정 지역 및 성별 등의 단순 인구

통계학적 정보의 프로필을 기반으로 하는 패션 아울렛 광고는 법적 효과를 가지거나 법적 효과와 유사한 중요한 효과를 가진 의사 결정이 아닐 수 있습니다.

- 또한, 성별이나 연령 등에 따라 서비스에서 보이는 상품 배치를 다르게 하는 것은 규제 대상이 아닙니다. 그러나, 검색 서비스를 제공하면서 특정 인종에게 차별적인 컨텐츠나 광고를 우선 배치한다면 이는 규제 대상으로 볼 수 있습니다.
- 특히, 타겟이 되는 정보주체의 취약성을 판단함에 있어 일반적으로는 개인에게 영향이 거의 없더라도 특정 취약 계층이나 특정 소수 집단, 특정 유형의 사람에게는 영향을 미칠 수 있다는 점에 주의해야 합니다.

  ※ [예시] 재정이 취약한 사람에게 온라인 도박 광고가 주기적으로 노출되는 경우 도박 사이트에 가입함으로써 잠재적으로 재정 상태가 더욱 악화될 여지가 있음

3.4 프로파일링 기반 자동화된 의사결정을 활용하는 업무의 근거를 확인하십시오.

▪ 앞서 살펴본 바와 같이 정보주체는 원칙적으로 프로파일링에 의한 자동화된 의사 결정(automated decision making)의 대상이 되지 않아야 합니다. 왜냐하면 개인에게 중요한 의사 결정이 인공지능의 자동화된 알고리즘에 의해 이루어지는 경우 개인이 특정한 재화나 서비스에 접근하는 것이 부당하게 제외되거나 차별 금지 원칙(the principle of non-discrimination)을 위배하는 결과를 야기할 우려가 있기 때문입니다.

※ 예를 들면, 개인에게 중요한 영향을 미치는 승진에 대한 의사 결정이 인공지능에 의해 자동화되어 이루어지고, 인공 지능의 알고리즘 내에 특정 인종은 특정 분야의 업무와 맞지 않는다는 내용이 포함되어 있다면, 그리고 인공 지능의 판단만으로 특정 인종을 특정 업무 배치에서 배제한다면, 이는 부당한 차별에 해당하기 때문입니다.

▪ 그러나, 정보통신기술 고도화에 따라 프로파일링을 전면 배제할 수 없고 적절한 프로파일링에 기반한 서비스가 이루어지는 경우 이에 따른 정보주체의 이익 또한 명시적으로 존재하는 것도 사실입니다.

▪ 정보주체는 프로파일링 등 오직 자동화된 개인정보의 처리에 근거한 결정의 대상이 되지 않을 권리를 가지고 있다고 GDPR은 명시하고 있으며, (법 제22조 제3항) 아울러 프로파일링이 가능한 경우를 다음의 세 가지로 이 규정하고 있습니다. (동조 제4항)

① 컨트롤러와 정보주체 간 계약의 체결이나 이행을 위해 필요한 경우입니다.

※ 구체적으로는 다음과 같은 경우가 해당됩니다.

- 의사 결정에서 잠재적으로 더 나은 일관성 또는 공정성이 있는 경우 : 인적 오류, 차별 및 권련 남용 가능성의 감소 등
- 고객이 재화나 서비스에 대한 지불을 못할 위험이 감소하는 경우 : 신용 평가 참조 등
- 단기간 내 신속한 결정을 통해 프로세스 생산성을 향상하는 경우 : 데이터의 양이 방대하여 수동 처리가 현실적으로 불가능한 경우 등

② 유럽 연합 또는 회원국 법률에 의해 승인되었고 동 법령이 정보주체의 권리와 자유, 정당한 이익을 위해 적절한 조치를 포함하고 있는 경우입니다.

※ 예를 들면, 사기나 탈세 감시 및 방지나 컨트롤러가 제공하는 서비스의 보안과 신뢰성 보장 등을 위한 경우가 해당됩니다.

③ 정보주체의 명시적 동의(explicit consent)에 의한 경우입니다.

- 정보주체의 명시적 동의(explicit consent)에 의한 경우에는 프로파일링 및 자동화 의사 결정이 가능합니다.
- 다만, 정보주체의 동의를 받아 프로파일링 기반 자동화된 의사 결정 프로세스를 운영하고자 하는 컨트롤러는 정보주체가 동의 내용을 명확히 이해하고 있다는 사실을 보여줄 필요가 있습니다. 모든 경우에 정보주체는 프로파일링을 통한 예상된 결과 및 이에 활용에 대한 충분한 관련 정보를 제공받아야만 합니다.

- 또한, 정보주체에게 선택의 여지없이 사실상 동의가 강제되는 경우는 프로파일링의 적법한 근거가 아닙니다.

※ 프로파일링에 대한 동의가 컨트롤러가 제공하는 서비스 이용의 선행 조건이거나 고용관계처럼 권력의 불균형이 있는 경우에는 동의를 받더라도 프로파일링의 근거가 될 수 없습니다.

3.5 정보주체의 권리 보장 절차를 마련하십시오.

(1) 정보를 제공받을 권리

▪ 컨트롤러는 자동화된 의사 결정에 대한 투명성 확보를 위해 정보주체가 쉽게 확인할 수 있도록 프로파일링에 대한 정보를 제공하여야 합니다.

① 자동화된 의사 결정의 발생 사실

② 자동화된 의사 결정에 활용되는 로직(logic)에 관한 유의미한 정보

※ 머신 러닝(machine-learning) 등 인공지능의 발전과 복잡성으로 자동화된 의사 결정이나 프로파일링에 대해 이해하는 것이 어려울 있습니다. 그러나 컨트롤러는 알고리즘에 대한 복잡한 설명이나 전체 알고리즘 공개보다는 의사 결정의 근거나 기준에 대해 간단한 안내 방안을 찾아야 합니다.

③ 중요성과 예상 결과

▪ 현재 혹은 미래의 정보 처리에 대한 정보와 자동화된 의사 결정이 정보주체에게 미치는 영향이 제시되어야 합니다. 정보주체가 동 정보를 쉽게 이해할 수 있도록 실제적이고 구체적인 예시가 함께 제시되어야만 합니다.

※ 정보주체의 용이한 이해를 돕기 위해 IT 기술을 활용하여 자동화된 의사 결정에 대한 설명을 시각적으로 구현하여 제공하는 것이 좋습니다.

참 고

[자동화된 의사 결정에 활용되는 로직(logic)에 관한 유의미한 정보의 사례]

■ 대출 심사를 위해 대출 신청자의 신용 등급을 평가하는 경우

① 개인 정보의 출처 : 신용 등급은 신용 평가 기관이나 컨트롤러가 직접 수집한 정보를 기반으로 계산된다는 사실

※ 정보주체로부터 직접 수집한 정보가 아닌 경우 개인정보 수집 출처를 정보주체에 추가로 제공(제14조제2항)

② 신용 등급 결정의 근거

③ 신용 평가 과정이 공정하고 책임 있는 대출 심사 결정을 위해 필요하다는 사실

④ 신용 등급 결정을 위한 주요 고려 사항의 상세 정보(특히 정보의 출처 및 관련성 등)

- 대출 신청 양식에 정보주체가 기재한 정보
- 연체 기록 등 과거 금융 서비스 이용 기록
- 사기 및 연체·파산 인력과 같은 공공 기관 기록

⑤ 정보주체에 사용된 신용 등급 계산 방식이 공정하고 효과적이며 편파적이지 않도록 정기적으로 확인하고 있다는 사실

[중요성과 예상 결과의 사례]

■ 보험회사가 자동화된 의사 결정 프로세스를 활용하여 고객의 운전 습관을 모니터링하고 이를 기반으로 보험료를 설정하는 경우

① 위험한 운전은 높은 보험료를 유발할 수 있다는 사실

② 급가속 및 급정거 등의 위험한 운전 습관을 가진 운전자와 보통의 운전자를 상호 비교하는 기능 제공

(2) 열람권

▪ 정보주체는 자동화 의사 결정에 관해 정보주체가 컨트롤러와 동일한 정보를 가질 권리를 보장해야 합니다. 이 경우 다음과 같은 사항이 포함되어야 합니다.

① 프로파일링을 포함한 자동화된 의사 결정 과정의 구현 사실
② 자동화된 의사 결정에 활용된 로직(logic)에 대한 유의미한(meaningful) 정보
③ 중요성 및 예상 결과

(3) 완전 자동화된 의사 결정의 대상이 되지 않을 권리

▪ 컨트롤러는 GDPR 제22조제2항에 근거하여 예외적으로 완전 자동화된 의사 결정을 수행하더라도 정보주체에게 의사 결정 과정에 인적 개입(human intervention)을 요구할 수 있는 권리와 도출된 결과에 대한 자신의 관점(point of view)를 표현할 수 있는 권리를 보장해야 합니다. 이를 위해 정보주체가 이와 같은 권리를 행사할 수 있는 간단한 방법을 제공해야 합니다.

▪ 이들 권리의 보장에서 가장 중요한 사항은 인적 개입(human intervention)의 보장입니다. 모든 검토 과정에는 적절한 권한과 역량을 갖춘 사람이 개입해야 합니다. 검토자는 정보주체가 제공한 추가 정보를 포함하여 의사 결정 과정에서 활용된 모든 데이터를 철저히 평가해야 합니다.

참 고

■ 제29조 작업반의 프로파일링 가이드라인에서는 위에 규정된 사항 외에 추가적인 데이터 주체의 권리를 규정하고 있습니다.

■ 제13조~제14조 정보를 제공받을 권리(Right to be informed)

- 투명성 확보를 위해 컨트롤러는 개인에게 프로파일링 또는 자동화 된 의사 결정 프로세스가 어떻게 작동하는지 명확하고 간단하게 설명해야합니다.
- 특히, 프로파일링에 기반한 의사결정이 발생하는 경우 GDPR에서 규정하는 요건과 자동화된 의사 결정 요건과는 무관하게 제5조제1항제a호에서 규정하는 투명성 확보 조치의 일환으로 ① 프로파일링 발생 사실과 ② 생성된 프로필을 데이터 주체에 명확하게 안내해야 합니다.(전문 제60조)
- 또한, 프로파일링 기반 의사 결정의 완전 자동화 여부와 무관하게 정보주체는

프로파일링에 관한 정보를 제공받을 권리와 프로파일링에 반대할 수 있는 권리(특정 상황에 제한)가 있습니다.

■ 제15조 열람권(Right to access)

- 정보주체는 프로필 생성에 활용된 정보의 범위 및 상세 항목, 결정 내용을 확인할 수 있습니다.
- 다만, 프로파일링과 관련 내용이 중요한 영업 비밀 혹은 지적 재산 공개할 우려가 있는 등 컨트롤러의 권리와 자유에 악영향을 미치는 경우에는 정보주체의 열람권이 제한될 수 있으나 이는 매우 드문 경우에만 해당되며 맥락과 정보주체 권리를 균형 있게 검토해야 합니다. (전문 제63조)
- 또한, 컨트롤러는 정보주체가 자신의 개인정보를 열람할 수 있는 안전한 원격 서비스를 제공해야 하고 프로파일에 대한 정보 외에도 프로필 작성을 위해 입력되는 정보 또한 열람 가능하도록 조치해야 합니다.

■ 제16조 정정권(Right to rectification)

- 프로파일링에는 부정확성을 증가할 수 있는 요소가 포함될 수 있습니다. 입력 데이터가 부정확하거나 상관성이 없거나 맥락에서 벗어날 수 있으며 이로 인해 상관관계 식별을 위한 알고리즘에 문제가 있을 수 있습니다. 따라서 정보주체는 사용된 데이터의 정확성 및 분류된 그룹 또는 카테고리에 대해 이의를 제기할 수 있습니다.
- 또한, 정보주체는 추가적인 정보 제공을 통해 개인정보를 보완할 수 있는 권리가 있습니다.
  ※ 예를 들어, 심장 질환 병력이 없는 특정 개인을 의료 기관의 시스템이 심장 질환 발생 가능성이 높은 그룹에 배치하는 경우 정보주체는 정보 처리 목적을 고려하여 추가적인 정보를 제공하거나 의료기관보다 더 높은 성능의 시스템 혹은 고급 통계 모델을 활용을 통해 의료 기관의 프로파일링 결과를 수정을 요구할 수 있는 권리가 있습니다.
- 수정 권한은 프로필 작성에 활용된 '입력된 개인정보'와 '출력 데이터'(프로필 자체 또는 해당 개인에게 할당된 '점수' 혹은 개인의 특성 등) 모두에 적용됩니다.

■ 제17조 삭제권(right to erasure) 및 제18조 처리제한권(right to restriction of processing)

- 삭제권 또한 입력 및 출력 데이터 모두에 적용됩니다. 특히, 프로파일링의 근거가 동의라면, 정보주체가 동의를 철회한 경우 컨트롤러는 프로파일링을 위한 다른 법적 근거가 없는 한 관련 개인정보를 모두 삭제해야 합니다.
- 처리 제한권 또한 프로파일링 과정의 모든 단계에 적용될 것입니다.

■ 제21조 반대권(Right to object)

- 제21조 제1항에 따라 정보주체는 프로파일링 및 자동화된 의사 결정에 반대할 수 있는 권리가 있습니다.

- 정보주체가 동 권리를 행사한 경우 정보주체의 이익이나 권리 및 자유에 우선하는 합법적 근거를 입증할 수 없는 한 프로파일링 과정에 개입하거나 중단해야 하며 경우에 따라 관련 정보를 삭제해야 합니다.
- 정보주체의 반대권을 제한할 수 있는 합법적 근거를 GDPR 상에 밝히고 있지 않으나 아래의 사례를 참고하십시오.
  ※ 예를 들어, 과학적 연구의 수행 혹은 전염성 질병의 확산 예측 등 컨트롤러의 비즈니스적 이익을 위해서가 아니라 프로파일링이 큰 틀에서 사회와 커뮤니티 대상 혜택을 제공하는 경우
- 컨트롤러는 또한 다음의 사항을 입증해야 합니다.
  ① 특정 반대 요구 수용을 위해서는 정보주체에게 미치는 영향이 최소한의 필요성으로 제한됨(프로파일링이 반대 요구 수용에 미치는 영향이 거의 없음)
  ② 정보주체의 반대가 조직에 매우 치명적임
- 컨트롤러의 이익 보장과 정보주체의 반대 제기 사이에 양형 평가를 해야 하는데, EU 지침(Directive)과는 달리 정보주체의 반대를 거절하는 합법적 근거에 대한 입증 책임은 정보주체가 아니라 컨트롤러에게 있습니다.
- 다만, 제21조제2항에 따라 다이렉트 마케팅 목적의 개인정보 처리에 대해서는 조건 없이 반대가 가능합니다. 프로파일링 또한 해당되는데 이 경우에는 영향 평가를 수행할 필요가 없으며 컨트롤러는 무조건 정보주체의 반대 요구를 수용해야 합니다.

3.6 민감정보와 아동의 개인정보가 처리되는지 확인하십시오.

(1) 민감정보 처리 제한

▪ 자동화된 의사결정 과정에서 민감 정보가 활용되어서는 안 됩니다. 민감 정보란 인종, 정치적 견해, 종교나 신념, 노동조합 가입 여부, 유전 또는 건강 상태, 성적 취향 등을 의미합니다.

▪ 다만, 정보주체의 명시적인 동의(explicit consent)가 있거나, EU 또는 회원국 법률에 기초한 상당한 공익 목적으로 처리가 필요한 경우에는 가능합니다. 그리고 이 과정에서도 정보주체의 권리와 자유를 보호하고 합법적 이익을 보장해야 합니다.

(2) 아동의 개인정보 처리 제한

▪ 프로파일링 기반 자동화된 의사결정은 아동에게 적용되어서는 안 됩니다(전문 제71조). 다만, 아동 복지 보호 등을 위해 자동화된 의사 결정을 수행해야 하는 경우에는 제22조 제2항에 근거하여 수행할 수 있습니다.

▪ 또한 법률 아동 대상 프로파일링 및 자동화된 의사 결정을 수행하는 경우에는 제22조제2항의 보호조치(safeguards) 등이 아동에게 적합한 방식으로 적용되어야 합니다. 컨트롤러는 이러한 보호조치가 데이터를 처리하는 아동의 권리, 자유, 정당한 이익을 보호하는데 효과적인지 확인 하여야 합니다.

▪ 또한, 아동은 사회적 취약 계층에 속하므로 기업에서 마케팅 목적으로 프로파일을 하는 것은 제한(refrain)되어야 합니다. 아동은 온라인 환경에서 특히 취약할 수 있고 행태 정보 기반 광고에 쉽게 영향을 받을 수 있습니다.

※ 예를 들어, 온라인게임에서 프로파일링은 알고리즘이 고려하는 플레이어를 목표로 삼아 게임에 돈을 쓰고 개인화된 광고를 제공하는데 사용될 수 있습니다. 아동의 연령과 지적 수준은 이러한 유형의 마케팅의 동기 또는 그 결과를 이해하는 능력에 영향을 줄 수 있습니다.

3.7 보호조치(safeguards)를 수립하십시오.

▪ 컨트롤러와 정보주체의 계약의 이행을 위해 필요한 경우나 정보주체의 동의를 받아 이루어지는 자동화된 의사 결정의 경우에는 보호조치(safeguard)를 수립해야 합니다.

- 보호조치(safeguard)에는 최소한 정보주체가 인적 개입을 요구할 수 있고, 의견을 표명하여 결정에 항의할 수 있는 방법이 포함되어야 합니다.

▪ 법령에 근거한 자동화된 의사결정의 경우에도 정보주체 대상 투명성 확보를 위해 적절한(suitable) 보호조치를 해야 합니다. 이는 보호조치(safeguard)와는 달리 다소 제한적입니다. 정보주체는 자동화된 의사 결정이 어떤 근거로 어떻게 이루어졌는지를 이해하는 경우 오직 결정에 항의하거나 의견을 표명할 수 있습니다.

▪ 수집·공유된 정보나 자동화된 의사 결정 과정의 오류 또는 편향성으로 인해 1) 정보주체의 분류가 잘못되거나 2) 부정확한 예측에 기반한 평가가 발생하거나 3) 개인에게 부정적 영향을 유발할 수 있습니다.

- 이를 방지하기 위해 컨트롤러는 데이터의 편향성 발생 여부를 수시로 평가하여 상관관계에 대한 과도한 의존 등 부적합한 요인에 대처할 수 있는 방법을 개발해야 합니다.

※ 알고리즘 감사 및 프로파일링·자동화 의사 결정 프로세스의 정확성과 상관성에 대해 주기적으로 검토하는 체계 구축 등이 유용한 방법입니다.

▪ 또한, 프로파일링 및 자동화된 의사 결정 과정에 민감 정보가 처리되어 오류, 부정확, 차별 발생 방지를 위한 절차와 조치를 도입하고 주기적으로 점검해야 합니다. 이 같은 조치는 설계단계에서도 고려되고 지속적으로 수행되어야 하며 점검 결과는 다시 시스템에 개선 반영되어야 합니다.

3.8 자동화된 의사 결정을 개인정보 영향평가(DPIA) 대상에 포함하십시오.

▪ 개인정보 영향평가(DPIA)의 평가 기준으로 자동화 의사 결정으로 인한 위험성을 포함해야 합니다. 다시 말해, 프로파일링을 포함한 자동화된 처리에 근거한 자연인에 대한 체계적이고 광범위한 평가(a systematic and extensive evaluation)가 이루어져야 합니다.

▪ 완전 자동화된 처리보다는 자동화된 처리에 '근거'한 프로파일링과 의사 결정에 대한 평가가 이루어져야 합니다.

▪ 개인정보 영향평가의 기준으로는 다음과 같은 사항이 추가로 고려될 수 있습니다.

① 자동화 된 의사 결정 프로세스와 관련된 논리 및 존재에 대해 정보주체 고지 여부
② 정보주체 대상 처리의 중요성 및 예상 결과 설명 여부
③ 정보주체 대상 자동화된 의사 결정 반대 수단 제공 여부
④ 정보주체 대상 견해를 표명할 권리 허용 여부

3.9 프로파일링에 GDPR 개인정보보호 원칙의 적용 여부를 확인 하십시오.

(1) 적법성, 공정성, 투명성 확보 (lawful, fair and transparent)

▪ 프로파일링 프로세스는 정보주체에게 직관적으로 보이지 않고 이해하기 어려우므로 간결하고 투명한 방법으로 정보주체가 알기 쉽게 개인정보 수집 단계에서 제공해야 합니다.

☞ **(예시)** 보험회사가 개인의 운전 습관에 따라 보험료를 차등 설정하는 경우 주행 거리, 주행 시간, 주행 경로 등의 정보를 수집하여 급가속 및 급정거 등의 부적절한 운전 습관 확인에 활용할 수 있음

▪ 또한, 보다 정확한 예측을 위해 날씨, 교통, 도로 유형 등의 다른 정보와도 결합 가능합니다. 컨트롤러는 수집된 정보, 자동화된 의사 결정 활용 사실, 관련 로직, 의사 결정의 중요성과 예상 결과 등을 정보주체에게 고지해야 합니다.

▪ 프로파일링은 특정 사람들에게 취업 기회를 박탈하거나 과도한 위험 혹은 비용 평가를 통해 타겟화 된 금융 상품의 접근, 신용 혹은 보험 가입에 있어 불공정한 결과나 차별을 유발할 수 있습니다.

▪ 데이터 브로커가 고객의 동의나 인지 없이 금융기관을 대상으로 고객의 취약한 재정 상태가 담긴 프로파일을 판매하고 금융기관이 이를 기반으로 해당 고객 대상 고금리 고위험 금융 상품을 판매하는 행위 등은 공정한 계약 행위로 보기 어렵습니다.

(2) 추가 처리와 목적 제한 (further processing and purpose limitation)

▪ 프로파일링은 최초 수집된 개인정보 외에 추가적 정보 사용을 유발할 수 있습니다.

☞ **(예시)** 위치 서비스로 할인 가능한 근처 음식점을 제안하는 모바일 앱의 경우 수집된 정보를 활용하여 음식 선호도 또는 라이프 스타일 식별 등 마케팅 목적의 프로파일링 생성에 활용 가능합니다.

- 위치 정보의 추가 이용은 최초 수집 목적과는 상이하므로 이에 대한 정보주체 추가 동의가 필요합니다.

▪ 추가 이용 여부에 대한 판단 근거는 아래 요건을 참고할 수 있습니다.

① 개인정보 수집 목적과 추후 처리 목적 간의 관계
② 개인정보 수집 맥락과 추후 사용에 대한 정보주체의 합리적인 기대.
③ 개인정보의 성격과 추가 처리가 정보주체에 미치는 영향
④ 공정성 보장 및 정보주체 대상 부당한 영향 방지를 위한 보호조치

(3) 데이터 최소화 (data minimization)

▪ 정보 기술 고도화에 따라 실제 필요한 정보보다 많은 데이터의 보유가 가능합니다. 컨트롤러는 개인정보의 수집•보유 필요성을 명확하게 설명하고 정당화 할 수 있어야하며 프로파일링을 위해 총계처리되거나 익명으로 처리 된 데이터 사용을 고려해야 합니다.

(4) 정확성(accuracy)

▪ 컨트롤러는 아래의 프로파일링 프로세스의 모든 단계에서 정확성을 고려해야 합니다.
① 정보의 수집 ② 정보의 분석 ③ 개인별 프로파일링의 수립
④ 개인에게 영향을 미치는 의사 결정시 프로파일링 적용

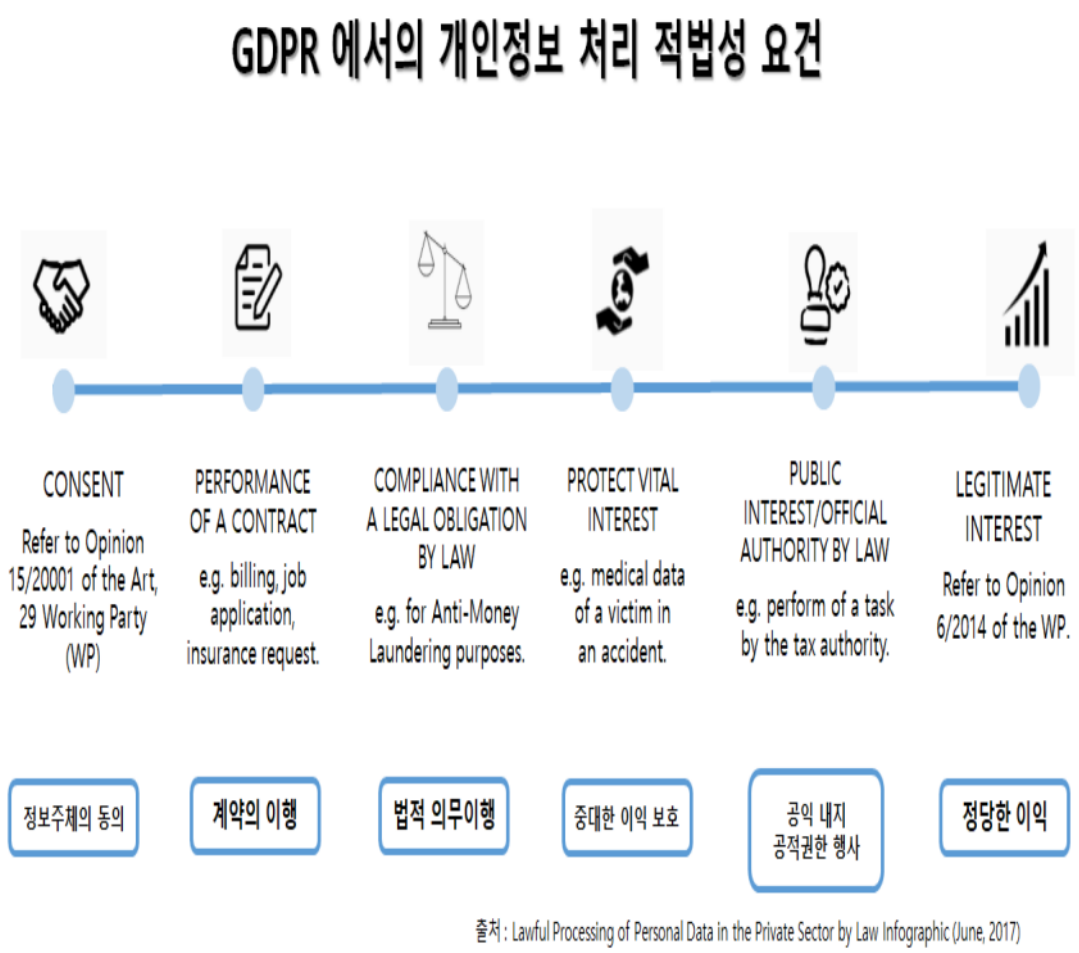
▪ 자동화된 의사 결정 및 프로파일링에 이용되는 정보가 부정확한 경우 도출되는 결론이나 프로필에 결함이 발생할 수 있습니다. 또한, 최신성이 확보되지 않은 정보 또는 잘못된 외부 정보는 개인의 건강, 신용, 보험상의 위험에 대한 부적절한 예측으로 이어질 수 있습니다. 분석 대상 데이터가 정확하게 기록되더라도 데이터 세트가 완전한 대표성을 가지고 있지 않거나 분석에 있어서 편견이 포함될 수 있습니다.

▪ 따라서, 컨트롤러는 자동화된 의사 결정 및 프로파일링에 활용되는 정보의 정확성 및 최신성을 지속적으로 확인하고 안내함으로써 정보주체가 부정확성을 교정하고 정보의 품질을 향상시킬 있도록 조치해야 합니다.

(5) 보유 기간 제한(storage limitation)

- 머신러닝 알고리즘은 다량의 정보를 처리하고 상관관계를 구축하도록 설계되어 있습니다. 수집된 개인정보를 장기간 저장하는 경우 알고리즘은 더 많은 데이터를 분석할 수 있어 보다 종합적인 프로필 구축이 가능합니다.
- 그러나, 정보 수집 목적에 부합하는 개인정보라 할지라도 지나치게 오래 저장하는 것은 법의 기본원리인 과잉 금지의 원칙 (the proportionality consideration ; 기본권을 제한함으로서 달성되는 공익과 침해되는 사익을 비교하여 전자가 후자보다 월등하여야 한다는 원리)과 충돌하여 개인의 프라이버시 권리를 침해하게 될 수도 있습니다.

- 또한, 개인정보를 너무 장기간 보관하면 개인에 대한 분석 및 도출 결과의 부정확성이 높아질 위험이 있으므로 불필요한 정보는 적정 시점에서 삭제해야 합니다.



꼭 알아두기

■ **프로파일링 기반 자동화된 의사 결정에 적용되는 일반 원칙은 다음과 같습니다.**

① 제5조제1항 개인정보 처리 원칙(Principles)
- 적법성, 공정성, 투명성 확보(lawful, fair and transparent)
- 추가 처리와 목적 제한(further processing and purpose limitation)
- 데이터 최소화(data minimization)
- 정확성(accuracy)
- 보유 기간 제한(storage limitation)

② 제6조1항에 처리의 적법성(Lawfulness of processing)
- 정보주체의 동의
- 정보주체와의 계약 이행이나 계약 체결을 위해 필요한 처리
- 법적 의무 이행을 위해 필요한 처리
- 정보주체 또는 다른 사람의 중대한 이익을 위해 필요한 처리
- 공익을 위한 임무의 수행 또는 컨트롤러에게 부여된 공적 권한의 행사를 위해 필요한 처리
- 컨트롤러 또는 제3자의 적법한 이익 추구 목적을 위해 필요한 처리(단, 그 이익이 정보주체의 이익, 권리 또는 자유가 그 이익보다 중요한 경우는 제외)

③ 제9조 민감정보(Special categories of data)

④ 제13조~제14조 정보를 제공받을 권리(Right to be informed)

⑤ 제15조 열람권(Right to access)

⑥ 제16조 정정권(Right to rectification)

⑦ 제17조 삭제권(Right to erasure)

⑧ 제18조 처리제한권(Right to restriction of processing)

⑨ 제21조 반대권(Right to object)

관련 조문 및 근거

- 제4조(정의)
- 제9조 (민감정보)
- 제13조~제14조(정보를 제공받을 권리)
- 제17조 삭제권(right to erasure)
- 제18조 처리제한권(right to restriction of processing)
- 제21조 반대권(Right to object)
- 제22조(자동화된 의사결정 및 프로파일링 관련 권리)
- 제35조(개인정보 영향평가)
- 전문 제63조
- 전문 제71조

집필진·자문·감수

연구책임기관	행정안전부 개인정보보호협력과
	한국인터넷진흥원 개인정보협력팀
집필진(가나다순)	김경하 제이앤시큐리티 대표
	김도엽 고려대 정보보호대학원 변호사
	성경원 SK인포섹 이사
	윤수영 이베이코리아 팀장
	이진규 네이버 이사
	정윤정 김·장 법률사무소 위원
	채승완 한국인터넷진흥원 단장
	황인표 한국인터넷진흥원 수석연구원
외부 자문	박훤일 경희대학교 교수
	함인선 전남대학교 교수