

우리  
기업을  
위한

## EU 일반 개인정보보호법 가이드북

우리  
기업을  
위한

## EU 일반 개인정보보호법 가이드북



# EU 일반 개인정보보호법 가이드북

우리  
기업을  
위한

# EU 일반 개인정보보호법

## 가이드북



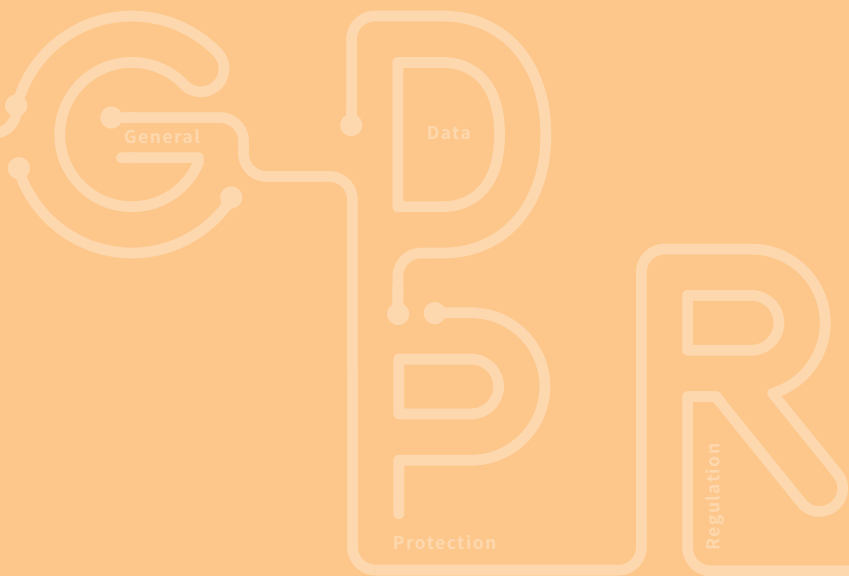


# EU 일반 개인정보보호법

## 가이드북



**EU 일반 개인정보보호법**  
가이드북



유럽연합은 2018년 5월 25일부터 개인정보 처리와 이동에 관한 “일반 개인정보보호법(GDPR)”을 본격 시행합니다. 이 법은 역내 자유로운 데이터의 흐름을 보장하고, 일관성 있는 규제환경을 마련함으로써 유럽연합의 디지털 단일 시장 환경을 조성하는데 기여할 것으로 기대되고 있습니다.

GDPR은 유럽연합내의 투자기업은 물론, 유럽연합 내 정보주체를 대상으로 하는 기업 활동에 폭넓게 적용되고, 정보주체의 권리와 처리자의 의무를 대폭 강화하도록 하고 있으며, 위반 시 막대한 과징금을 부과함으로써 우리 기업 활동에 부정적인 영향을 줄 것이라는 우려가 있는 것도 사실입니다.

그러나 우리는 GDPR을 규제 장벽으로만 인식할 것이 아니라, 개인 정보보호 컴플라이언스 수준을 다시금 점검하는 계기로 활용하는 지혜 또한 필요합니다. 즉 이를 통해 기업은 스스로 개인정보 보호역량을 강화하고, 안전하게 개인정보를 활용하여 기업의 가치와 소비자들의 신뢰도를 높일 수 있습니다.

전 세계 개인정보 이용과 활용에 있어 새로운 패러다임으로 부상한 GDPR을 올바르게 이해하고 그 대응력을 높인다면, 우리는 데이터의 안전한 활용이 화두인 4차 산업혁명을 더욱 능동적이고 선제적으로 이끌어 나갈 수 있습니다.

단기적으로 유럽연합 시장 진출 기회 확대는 물론, 글로벌 디지털 경제의 선봉에 설 수 있는 또 다른 기회를 맞이할 수도 있습니다.

부족하지만 본 가이드북이 GDPR을 올바로 이해하고 대응하는데 도움이 되기를 바라며, 제언이나 수정이 필요한 사항이 있으신 경우 언제든지 문의하시기 바랍니다.

고맙습니다.

## CONTENTS

---

### I 개요

1. 가이드북 발간 배경과 목적 .....	10
2. GDPR 시행에 따른 주요 변화 .....	12
3. GDPR 내 주요 용어 .....	19

---

### II GDPR 인식 제고와 준비

1. 제정 목적과 법적 성격 .....	34
2. GDPR의 구성 체계 .....	37
3. 적용 대상과 범위 .....	38

---

### III 주요 원칙

1. 개인정보 처리 원칙(Principles) .....	44
2. 처리의 적법성(Lawfulness of processing) .....	47
3. 동의(Consent) .....	49
4. 아동 개인정보(Children's personal data) .....	57
5. 민감정보 및 범죄행위 관련 정보(Special categories of personal data & Personal data relating to criminal convictions and offences) .....	61

---

### IV 컨트롤러·프로세서의 역할

1. 컨트롤러(Controller) .....	70
2. 대리인(Representatives) .....	72
3. 프로세서(Processor) .....	74

## V 정보주체 권리 강화

1. 개요	80
2. 정보를 제공받을 권리(Right to be informed)	81
3. 정보주체의 열람권(Right of access by the data subject)	85
4. 정정권(Right to rectification)	88
5. 삭제권(‘잊힐 권리’)[Right to erasure(‘Right to be forgotten’)]	90
6. 처리 제한권(Right to restriction of processing)	92
7. 개인정보 이동권(Right to data portability)	95
8. 반대권(Right to object)	98
9. 프로파일링을 포함한 자동화된 의사결정 (Automated individual decision-making, including profiling)	101

## VI 기업의 책임성 강화

1. 개요	112
2. 개인정보 처리 활동의 기록(Records of processing activities)	113
3. Data protection by design and by default	115
4. 개인정보 영향평가(Data protection impact assessment)	117
5. DPO(Data Protection Officer) 지정	123
6. 행동규약과 인증(Codes of conduct and certification mechanism)	128

## VII 개인정보 역외 이전

1. 개인정보 역외 이전(Transfers of personal data to third countries or international organizations)	142
---	-----



---

## VIII 개인정보 침해 발생 시 조치 사항

1. 개인정보 침해(Personal data breach) .....	156
2. 개인정보 침해 통지(Data breach notification) .....	159

---

## IX 피해 구제 및 제재 규정

1. 구제 제도(Remedies) .....	170
2. 손해배상권 및 책임(Right to compensation and liability) .....	172
3. 과징금(Administrative fines) .....	174
4. 벌칙(Penalties) .....	176

---

## X 참고 자료

1. GDPR 적용 대상 국가의 감독기구 현황 .....	184
2. 주요 질의 및 답변(Q&A) .....	189
3. 사업자를 위한 EU 집행위원회의 7단계 체크리스트 .....	197

## 표 목차

[표 1]	제29조 작업반 발표 보고서	11
[표 2]	개인정보와 개인정보가 아닌 정보	21
[표 3]	GDPR의 구성 체계	37
[표 4]	EU 회원국의 친권자 동의가 필요한 아동 연령	58
[표 5]	정보주체의 권리 강화에 대한 내용 및 관련 주요 조문	80
[표 6]	기업의 책임성 강화와 관련한 내용 및 조문	112
[표 7]	개인정보 처리 활동의 기록 내용	114
[표 8]	적정성 평가 절차	144
[표 9]	개인정보 침해 유형과 사례	157
[표 10]	개인정보 침해에 대한 감독기구 통지 필요 여부 판단 예시	165
[표 11]	개인정보 침해에 대한 정보주체 통지 불필요 예시	165

## 그림 목차

[그림 1]	EU의 법 체계	35
[그림 2]	GDPR의 개인정보 영향평가 수행 단계 흐름도	121
[그림 3]	DPO 지정 시 고려사항	132
[그림 4]	개인정보 처리 시 높은 위험의 판단 기준	136
[그림 5]	개인정보 역외 이전 메커니즘	143
[그림 6]	개인정보 역외 이전 흐름도	147
[그림 7]	개인정보 침해 통지 흐름도	163



# I. 개요

---

1. 가이드북 발간 배경과 목적
2. GDPR 시행에 따른 주요 변화
3. GDPR 내 주요 용어

# 1

## 가이드북 발간 배경과 목적

### Point

- GDPR 시행에 따른 주요 변화를 알 수 있다.

### 1.1 발간 배경

2016년 5월 유럽연합(이하 'EU')에서 제정한 「일반 개인정보보호법(General Data Protection Regulation)」(이하 'GDPR')이 2년간의 유예 기간 종료에 따라 2018년 5월 25일 본격 적용되었다.

GDPR은 기존의 EU 개인정보보호 지침인 「1995년 개인정보보호 지침(Data Protection Directive 95/46/EC)」(이하 'Directive')을 대체하며, 기존 Directive보다 강력한 제제가 예상된다.

이에 한국인터넷진흥원은 행정안전부와 함께 『우리 기업을 위한 '유럽 일반 개인정보보호법(GDPR)' 안내서』(2017. 4.)와 『우리 기업을 위한 '유럽 일반 개인정보보호법(GDPR)' 1차 가이드라인』(2017. 11.)을 우선 발간하여 우리 기업에게 필요한 GDPR 제정 취지와 주요 내용을 알기 쉽게 제시하고, GDPR 시행 이전에 기업들의 사전 조치 수준을 제고하는 데 도움을 주었다.

이 가이드북에서는 위 '안내서'와 '1차 가이드라인'에서 다루고 있는 GDPR 관련 내용 전반을 통합하여 독자의 정보 접근성을 높이고, EU의 정책 자문 기구인 'The Article 29 Data Protection Working Party'<sup>1)</sup>(이하 '제29조 작업반')에서 발표한

1) 제29조 작업반(The Article 29 Working Party, WP29): Directive에 의거해 설립된 '데이터 보호 작업반(Data Protection Working Party)'의

보고서(가이드라인, 의견서 등) 내용을 아우르면서 구체적인 사례와 참고 자료를 제시하고자 한다.

**[표 1] 제29조 작업반 발표 보고서**

순번	내용	채택	최신 개정
1	개인정보 이동권(The right to data portability)	2016. 12. 13.	2017. 4. 5.
2	DPO 임명(Data Protection Officer)	2016. 12. 13.	2017. 4. 5.
3	선임 감독기구(The lead supervisory authority)	2016. 12. 13.	2017. 4. 5.
4	개인정보 영향평가와 높은 위험을 내재한 개인정보의 처리 [Data Protection Impact Assessment(DPIA) and determining whether processing is 'likely to result in a high risk']	2017. 4. 4.	2017. 10. 4.
5	과징금 부과 (The application and setting of administrative fines)	2017. 10. 3.	-
6	개인정보 침해 통지(Data breach notification)	2017. 10. 3.	2018. 2. 6.
7	자동화된 의사결정 및 프로파일링 (Automated decision-making and profiling)	2017. 10. 3.	2018. 2. 6.
8	동의(Consent)	2017. 11. 28.	2018. 4. 16.
9	투명성(Transparency)	2017. 11. 29.	2018. 4. 11.
10	인증기관에 대한 인정 (Accreditation of certification bodies)	2018. 2. 6.	-
11	제49조, 역외 이전 시 특정 상황에 대한 예외 조항 (Article 49, Derogations for specific situation)	2018. 2. 6.	-

## 1.2 발간 목적

이 가이드북은 GDPR의 본격적인 시행에 맞추어 GDPR이 규정하는 법에 대한 세부 지침, 주요 개념의 해석, 정보주체의 권리 강화를 위한 권리의 명시, 기업의 책임성 강화를 위한 내부 관리 기법 등의 내용을 우리 기업이 쉽게 이해하고 숙지할 수 있도록 작성되었다.

또한 우리 기업이 GDPR의 전반적인 이해를 통하여 기업 생태계에 맞는 개인정보보호 기반을 구축하고 글로벌 시장에서 경쟁력을 제고하는 데 기여하고자 한다.

약칭으로, EU 집행위원회에게 데이터 보호 관련 사안에 대한 조언을 제공하고, EU 회원국들이 조화로운 데이터 보호 정책을 추진할 수 있도록 지원한다(출처: 유럽 개인정보보호 감독관, [https://edps.europa.eu/data-protection/data-protection/glossary/a\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/a_en)). 제29조 작업반은 GDPR 시행과 함께 유럽 개인정보보호 이사회(European data protection board, EDPB)로 대체된다(전문 139항).

## 2

# GDPR 시행에 따른 주요 변화

### 2.1 적용 범위의 확립

EU 내 설립된 기관의 개인정보 처리 활동 외에 다음 경우를 적용 범위에 포함하였다.

- ① EU 밖에서 EU 내에 있는 정보주체에게 재화나 용역을 제공하는 경우
- ② 또는 EU 내에 있는 정보주체가 수행하는 활동을 모니터링하는 기관

※ 이 때, 유럽 경제 지역(European Economic Area, EEA)에 관한 주요 협정 제7조(a)에 따라 아이슬란드, 리히텐슈타인, 노르웨이도 EU와 동등하게 GDPR이 적용된다고 본다.

### 2.2 개인정보 정의의 확립

기존 Directive에 명시되지 않았으나 판례, 유권해석, 개별법 차원에서 인정된 개념을 개인정보로 포함하였다.

- ① 개인 식별이 가능한 경우의 IP 주소, 쿠키(cookie) ID, RFID(무선 인식) 태그 등을 개인정보(온라인 식별자)에 포함한다(전문 제30항).
- ② 위치정보는 개인정보의 한 유형으로 소개된다(제4조제1항).
- ③ 민감한 성격의 개인정보를 '특별한 유형의 개인정보'(이하 '민감정보')라고 정의하면서, 유전정보와 생체 인식정보를 포함한다(제9조제1항).

- ④ 개인정보의 가명처리(pseudonymisation) 개념을 도입하였고(제4조제5항), 이를 적용하는 경우 Data protection by design and by default의 이행 등 다양한 실익을 거둘 수 있게 하였다.

## 2.3 개인정보 기본 처리 원칙의 확립

개인정보를 처리하는 경우 다음 7가지 원칙을 모두 준수하여야 한다(제5조).

- ① (처리) 적법성·공정성·투명성 원칙
- ② (수집) 목적 제한의 원칙
- ③ 개인정보 처리의 최소화 원칙
- ④ 정확성의 원칙
- ⑤ 보유 기간 제한의 원칙
- ⑥ 무결성과 기밀성의 원칙
- ⑦ 책임성의 원칙

## 2.4 아동 개인정보 동의 원칙의 확립

만 16세 미만의 아동에게 직접 정보사회서비스를 제공할 때 부모 등 친권을 보유하는 자의 동의를 받아야 한다.

다만 각 회원국은 개별 법률을 통하여 친권자 동의를 요하는 아동의 연령 기준을 만 13세까지 낮추어 규정할 수 있다.

## 2.5 적법 처리 기준의 상향

개인정보 처리의 적법성·공정성·투명성 원칙에 따라 개인정보 처리는 GDPR에서 허용한 다음 중 어느 하나 이상의 요건에 해당해야 적법 처리로 인정된다(제6조).



- ① 정보주체가 하나 이상의 특정한 목적을 위하여 본인의 개인정보 처리에 동의한 경우
- ② 정보주체가 계약 당사자로 있는 계약의 이행을 위하여 또는 계약 체결 전 정보주체의 요청에 따라 조치를 취하기 위하여 처리가 필요한 경우
- ③ 컨트롤러에 적용되는 법적 의무를 준수하는 데 처리가 필요한 경우
- ④ 정보주체 또는 제3자의 중대한 이익을 보호하기 위하여 처리가 필요한 경우
- ⑤ 공익상의 이유 또는 컨트롤러에게 부여된 직무권한을 행사할 때 처리가 필요한 경우
- ⑥ 컨트롤러의 정당한 이익을 달성하기 위하여 처리가 필요한 경우

## 2.6 one-stop-shop 메커니즘<sup>2)</sup>의 도입

컨트롤러와 프로세서는 여러 국가에 흩어져 있는 정보주체의 개인정보 처리에 대하여 하나의 감독기구(선임 감독기구)를 대상으로 대응이 가능하다(제56조, 전문 제127항).

각 감독기구는 GDPR 위반이 한 회원국의 사업장에만 관련이 있거나 해당 회원국의 정보주체에 중대한 영향을 미치는 경우 선임 감독기구에 관련 사항을 통지해야 하며, 내용을 통지받은 선임 감독기구는 해당 감독기구가 자체적으로 사안을 처리할 것인지 선임 감독기구에서 해당 사안을 처리할 것인지 결정해야 한다. 이 때 선임 감독기구가 해당 사안을 처리하는 경우 이 역시 one-stop-shop 메커니즘이 작동한 것으로 본다.

## 2.7 프로세서에게도 다수의 규정이 직접 적용

기존 Directive와 달리 프로세서를 직접 규제하는 다음 내용을 다수 포함하고 있다.

---

2) one-stop-shop 메커니즘: 처리되는 개인정보의 정보주체가 EU 내 여러 국가에 흩어져 있는 경우 주 사업장이나 단일 사업장이 소속된 국가의 감독기구가 선임 감독기구의 역할을 수행하면서 다른 회원국의 감독기구와 수시로 협력함으로써 컨트롤러·프로세서는 하나의 감독기구만을 대상으로 대응 가능한 메커니즘.

- ① 처리활동의 기록(제30조)
- ② 개인정보 처리 보안 기준 적용(제32조)
- ③ 정기적인 개인정보 영향평가 수행(제35조)
- ④ 제3국 및 국제기구로의 개인정보 역외 이전(제5장)
- ⑤ 국가 감독기구 협조 의무(제31조) 등

또한 프로세서는 제재의 직접적 적용 대상이 되며(제83조), GDPR 요구 사항을 충족하지 못할 경우 정보주체로부터 배상을 요구받을 수 있다(제79조).

## 2.8 정보주체의 권리 확대

- ① 열람권(제15조)
- ② 정정권(제16조)
- ③ 삭제권(제17조)
- ④ 처리 제한권(제18조)
- ⑤ 개인정보 이동권(제20조)
- ⑥ 반대권(제21조)
- ⑦ 프로파일링을 포함한 자동화된 의사결정의 대상이 되지 않을 권리(제22조) 등

## 2.9 책임성과 거버넌스 강화

- ① 처리 활동의 기록(제30조)
- ② 높은 위험(high risk)을 내재한 개인정보 처리에 대하여 개인정보 영향평가 수행(제35조)
- ③ DPO(Data Protection officer) 지정(제37조)
- ④ 개인정보 침해 통지 및 종합적 기록 유지(제33~34조)
- ⑤ Data protection by design and by default 이행(제25조) 등

## 2.10 DPO(Data Protection Officer) 의무 지정

다음에 해당하는 경우 DPO를 의무로 지정해야 하며, DPO는 조직이 개인정보보호 의무를 준수하도록 도움을 줄 수 있다.

- ① 정부부처 또는 관련기관이 개인정보를 처리하는 경우(법원은 예외)
- ② 컨트롤러나 프로세서의 핵심 활동이 다음에 해당하는 경우
  - 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링에 해당하는 활동
  - 민감정보나 범죄경력 및 범죄행위에 대한 대규모 처리인 활동

## 2.11 개인정보 역외 이전 메커니즘 확립

EU는 EU 내 수집된 개인정보의 역외 이전을 원칙적으로 금지하지만, EU가 인정하는 메커니즘에 따라 역외 이전을 허용한다.

- ① 적정성 결정(adequacy decision)을 통하여 개인정보보호 관련 법제가 적절한 수준의 보호를 보장하고 있다고 인정된 나라로 이전하는 경우
- ② '적절한 보호조치(appropriate safeguards)의 제공', '정보주체의 권리 행사 보장', '효과적인 법적 구제 수단의 존재'에 모두 해당하는 경우
  - 적절한 보호조치에는 구속력 있는 기업 규칙(Binding Corporate Rules), 표준 개인정보보호 조항(Standard data protection clauses), 승인된 행동규약(Code of Conduct) 및 인증(Certification) 등이 포함
- ③ 위의 메커니즘에 해당하지 않더라도 명시적 동의(explicit consent), 계약의 이행 또는 정보주체의 요청으로 필요한 경우, 공익의 중요한 이유 등과 같은 특정 상황에서 예외 요건에 해당하는 경우에 역외 이전이 가능하다(제49조).

## 2.12 개인정보 침해 통지 제도의 확대

컨트롤러는 개인의 권리와 자유에 위협을 일으킬 가능성이 있는 침해가 발생한 경우,

개인정보 침해 사실을 인지한 시점으로부터 72시간 내에 감독기구에 신고하여야 하며, 개인의 자유와 권리에 높은 위험이 예상될 때에는 가능한 한 신속하게(without undue delay) 침해 사실을 정보주체에게 통지하여야 한다.

다만 개인정보 침해가 개인의 권리와 자유에 위험을 일으킬 가능성이 낮은 경우 통지하지 않을 수 있다.

※ 개인정보가 이미 공개되어 있고, 이러한 정보의 공개가 개인에 대한 위험을 일으킬 가능성이 없는 경우, 컨트롤러가 적절한 기술적·관리적 보호조치를 이행한 경우 (특히 암호화한 경우), 정보주체의 권리와 자유에 높은 위험이 발생하지 않도록 보장하는 후속 조치를 취한 경우 등

프로세서는 개인정보 침해 사실을 알게 된 때 컨트롤러에게 그 사실을 가능한 한 신속하게(without undue delay) 알려 주어야 한다.

## 2.13 제재 규정의 강화

각각의 개인정보 처리에 따라 제재 규정을 적용하며, '사업체 그룹' 매출을 바탕으로 과징금(fines imposed by reference to the revenues of an undertaking)을 부과한다.

- ① GDPR 규정의 일반적 위반의 경우 직전 회계연도의 전세계 매출액 2% 또는 1천만 유로 중 더 큰 금액
- ② GDPR 규정의 심각한 위반의 경우 직전 회계연도의 전세계 매출액 4% 또는 2천만 유로 중 더 큰 금액

## 2.14 인증제도 및 인증기관에 대한 인정 규정

GDPR은 인증을 발급하는 인증기관(certification bodies)이 소관 감독기구

(competent supervisory authority)나 국가의 인정 기관(national accreditation body), 또는 두 기관 모두의 인정을 받도록 요구하고 있다.

이는 인증 메커니즘 수립과 개인정보보호를 보장하기 위한 것으로, 효과적인 인증 메커니즘을 도입할 경우 GDPR 준수와 정보주체에 대한 투명성 향상 효과를 제공할 것으로 기대된다.

# 3

## GDPR 내 주요 용어

### Point

- GDPR에서 제시된 주요 용어의 개념을 이해할 수 있다.

### 3.1 주요 용어의 표기

이 가이드북은 앞서 발간된 ‘안내서’와 ‘1차 가이드라인’에서 표기한 용어를 준용하는 것을 원칙으로 하나, GDPR에 명시된 내용에 따라 변경되어야 할 필요성이 있는 용어는 고치는 것으로 하였다.

※ Directive 제26조제2항에 사용된 ‘표준 계약 조항(Standard Contractual Clauses)’의 경우 제46조2항(c)에 명시된 ‘표준 개인정보보호 조항(Standard Data Protection Clauses)’의 표현을 우선 사용하였다.

GDPR에서 사용하는 용어가 우리나라 개인정보보호 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 by default 등)하였다.

※ DPO란 Data Protection Officer의 약자로 조직이 개인정보보호 관련 법률을 준수하고 개인정보보호 의무를 다하도록 조언 및 도움을 주는 역할을 한다. DPO는

내부 직원 또는 외부 인사로 지정할 수 있다.

※ EU GDPR 제37조에서 명시하는 'DPO'와 우리나라 개인정보보호법 제31조의 '개인정보 보호책임자'는 지정 요건, 책무, 자격, 업무 독립성, 고용 형태 등이 서로 다른 직위이므로 영어 약어를 그대로 표기하였다.

※ Data protection by design and by default의 경우 우리말로 번역했을 때 생길 수 있는 혼동을 방지하고자 영어 원문을 그대로 표기하였다.

또한 다음의 경우 명확한 의미 전달을 위하여 한글·영문을 병기하여 표기하는 것을 원칙으로 하였다.

① 중요한 용어이거나 한글·영문을 병기할 때 의미 전달이 더 정확하고 효율적인 경우[예: 보호조치(safeguard), 민감정보(special categories of personal data) 등]

② 우리말로 번역하여 그 의미 범위가 넓게 또는 좁게 전달될 수 있는 경우[예: 가명처리(pseudonymisation), 열람권(right of access by the data subject) 등]

※ pseudonymisation은 가명화 또는 가명처리로 해석될 수 있으나, GDPR에서 명시하는 pseudonymisation은 보호조치 수단으로서의 '처리'를 의미하기 때문에 과대 해석될 수 있는 '가명화'보다 '가명처리'라는 용어를 우선 사용하였다.

※ right of access는 접근권이라고 해석하기도 하나, 정보에 대한 공개는 단순 접근이 아닌 정보주체의 자발적인 요청과 이를 통한 열람을 내포하기 때문에 '열람권'이라는 용어를 우선 사용하였다.

## 3.2 주요 용어의 정의(제4조)

### 3.2.1 개인정보(Personal data)(제4조제1항)

'개인정보'란 식별되었거나 또는 식별 가능한 자연인(정보주체)과 관련된 모든 정보를 의미한다.

GDPR은 기존 Directive에 명시적으로 기재하지 않았던 온라인 식별자, 위치정보, 유전정보 등을 개인정보에 포함함으로써 개인정보의 개념을 확립하고 있다. 이 때 개인정보의 형태는 문자에 한정하지 않고 특정 개인을 나타내는 음성, 숫자, 그림, 사진 등의 형태를 포함한다.<sup>3)</sup>

그 예로 개인을 직접 또는 간접적으로 식별 가능한 경우라면, 이름·전화번호 등과 같은 일반적인 개인정보 외에 온라인 식별자<sup>4)</sup>나 위치정보도 GDPR이 정의하는 개인정보에 해당한다.

**[표 2] 개인정보와 개인정보가 아닌 정보<sup>5)</sup>**

개인정보	개인정보가 아닌 정보
① 이름(name)과 성(surname)	① 사업자등록번호
② 주소	② info@company.com과 같은 형식의 이메일
③ name.surname@company.com과 같은 형식의 이메일 주소	주소(개인 메일이 아닌 업무용 공용 메일 등으로 활용되는 이메일 주소)
④ ID 카드 번호	③ 익명처리된 정보
⑤ 위치정보	
⑥ 쿠키 ID	
⑦ 광고 식별자(IDFA 또는 advertising identifier)	
⑧ 개인을 고유하게 식별할 수 있는 병원 및 의사가 보유한 데이터	

### 3.2.2 컨트롤러(Controller)(제4조제7항)

컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 주체를 의미하며, 이와 같은 결정은 컨트롤러 단독으로 하거나 또는 제3자와 공동으로 할 수 있다.

자연인을 비롯하여 법인, 정부부처 및 관련기관, 기타 단체 등이 컨트롤러가 될 수 있다.

3) 제29조 작업반(2007. 4.), Opinion 4/2007 on the concept of personal data, pp.7-8.

4) 온라인 식별자의 예시로 식별인자 및 기타 정보와 결합하여 개인 식별이 가능한 경우의 IP 주소, MAC 주소, 온라인 쿠키 ID, RFID 등이 포함된다(전문 제30항).

5) EU 집행위원회, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).



이 때 개인정보 처리의 목적과 수단이 EU 또는 회원국(Member state)의 법률에 의해 결정되는 경우, 컨트롤러 또는 컨트롤러 지정을 위한 기준은 EU 또는 회원국의 법률에 의해 정의될 수 있다.

### 3.2.3 프로세서(Processor)(제4조제8항)

프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 자연인, 법인, 정부부처 및 관련기관, 기타 단체 등을 의미한다.

프로세서는 컨트롤러의 지시에 따라 개인정보를 처리하며, 이 때 컨트롤러는 반드시 구속력 있는 서면 계약에 의해 프로세서를 지정하여야 한다.

### 3.2.4 수령인(Recipient)과 제3자(Third party)(제4조제9~10항)

수령인은 제3자인지 여부와 관계 없이 개인정보를 공개·제공받는 자연인이나 법인, 정부부처 및 관련기관, 기타 단체 등을 의미한다.

※ 예외적으로 EU 또는 회원국 법률에 따라 특정한 문의·회신 및 조회 업무를 수행하는 상황에서 개인정보를 제공받는 정부부처 및 관련기관(예: 세관 당국이나 금융 시장 규제 당국)은 수령인에 해당하지 않는다.

컨트롤러는 정보주체에게 그들의 개인정보가 어떤 수령인에게 공개·제공되었는지 알려 주어야 하는 의무를 부담하므로, 수령인 또는 수령인의 유형을 사전에 식별할 필요가 있다.

제3자는 ① 정보주체, ② 컨트롤러·프로세서, ③ 컨트롤러·프로세서의 직접적 권한에 따라 개인정보를 처리할 수 있는 개인을 제외한 모든 자연인이나 법인, 정부부처 및 관련기관, 기타 단체 등을 의미한다.

### 3.2.5 프로파일링(Profiling)(제4조제4항)

프로파일링은 개인의 특징을 분석하거나 예측하는 등 해당 개인의 특성을 평가하기 위하여 행해지는 모든 형태의 '자동화된(automatic)' 개인정보 처리를 의미한다.

예를 들면 개인의 업무 수행, 경제적 상황, 관심사, 지역적 이동 등을 분석하거나 예측하기 위하여 개인정보를 자동화된 방식으로 처리하는 경우 프로파일링에 해당한다.

컨트롤러는 프로파일링의 경우에도 GDPR의 개인정보보호 원칙에 따른 보호조치를 취해야 하며, 프로파일링에 사용된 개인정보와(input personal data) 프로파일링 결과 생성된 정보(output data) 모두에 정보주체의 권리를 보장해야 한다.

프로파일링을 통한 민감정보의 처리는 제9조제2항, 민감정보 처리 규정이 준수된 경우에만 가능하며 프로파일링을 포함한 자동화된 의사 결정에는 제22조를 통해 추가적인 보호조치를 적용해야 한다.

### 3.2.6 가명처리(Pseudonymisation)(제4조제5항)

정보의 처리에 대하여 추가적 정보를 사용하지 않고는 더 이상 원래의 개인정보를 알아볼 수 없는 상태로 만드는 것을 가명처리라고 한다.

이 때 추가적 정보는 분리 보관하여야 하고, 해당 정보를 이용하여 개인을 식별할 수 없도록 기술적·관리적 조치를 취하여야 한다.

GDPR에서 가명처리를 거친 정보는 추가적 정보의 사용을 통하여 개인 식별 가능성이 있으므로, 개인정보로 본다(전문 제26항).

개인정보를 가명처리하는 경우, 해당 기업은 ① data protection by design, data protection by default 의무를 충족하는데 도움이 되고, ② 개인정보를 보호할 수 있는 보안적 수단으로서의 장점 등을 가질 수 있다.

### 3.2.7 정보사회서비스(Information society service)(제4조제25항)

정보사회서비스는 Directive(EU) 2015/1535 of the European Parliament and of the Council의 제1조제1항(b)에서 정의한 서비스로, 서비스를 제공받는 자의 개별적 요청에 따라 원격에서 전자적 수단을 통하여 통상 영리 목적으로 제공되는 서비스를 의미한다.

- ※ 원격(at a distance): 서비스 제공자와 해당 서비스를 제공받는 자가 동시에 물리적으로 같은 장소에 있을 것을 요구하지 않는다.
- ※ 전자적 수단을 통하여(by electronic means): 전자적 장비로 데이터를 처리하여 서비스가 제공되는 것을 의미한다.
- ※ 서비스를 제공받는 자의 개별적 요청에 따라(at the individual request of a recipient of services): 개별적 요청을 바탕으로 한 데이터 전송에 의해 서비스가 제공되는 것을 의미한다.

정보사회서비스는 전자상거래서비스와 같이 온라인에서 재화와 용역을 사고파는 서비스에 한정되지 않으며, 상업적 목적으로 운영되는 모든 웹사이트가 정보사회서비스에 해당할 수 있다.

- ※ 온라인 광고를 통하여 수익을 창출하는 미디어 사이트, 검색 광고를 통하여 영리를 추구하는 검색엔진 등

### 3.2.8 감독기구(Supervisory authority)(제4조제21~22항)와 선임 감독기구(Lead supervisory authority)

#### 감독기구

GDPR은 EU 회원국마다 하나 이상의 감독기구(Supervisory Authority 또는 Data Protection Authority)를 의무 설립하도록 함으로써 컨트롤러와 프로세서의 개인정보 처리 활동에 대한 공조와 통제가 가능하도록 하고 있다.

감독기구는 다음 사유에 해당하는 경우 컨트롤러 또는 프로세서의 개인정보 처리에 관여한다.

- ① 컨트롤러나 프로세서가 자국 영토에 설립한 사업장에서 활용 중인 정보 처리
- ② 공익을 위하여 정부부처 및 관련기관이나 민간기구가 시행하는 정보 처리
- ③ 자국 영토의 정보주체에 영향을 미치는 정보 처리
- ④ EU 역내에 설립되지 않는 컨트롤러나 프로세서가 본인이 속한 국가에 거주하는 정보주체를 대상으로 시행하는 정보 처리 등(전문 제122항)

GDPR은 본문 전반에 걸쳐 다음과 같이 감독기구의 업무와 권한을 명시하고 있다(제57조).

- ① 컨트롤러와 프로세서와의 협력
- ② 영향평가의 수행 등에 대한 자문
- ③ 개인정보 침해 통지에 대한 신고 접수 및 민원 처리
- ④ 개인정보 침해 대책에 대한 지침 마련
- ⑤ 제28조제8항 및 제46조제2항(d)의 표준 개인정보보호 조항의 채택
- ⑥ 개인정보 역외 이전에 대한 고지 접수
- ⑦ GDPR 시행과 관련한 조사 실시
- ⑧ 개인정보보호 관련 위험, 규칙, 안전 조치 및 권리에 대한 공공 의식의 향상
- ⑨ 감독기구 간 상호 협력 등

감독기구는 업무 수행과 권한 행사에서 완전한 독립성을 가져야 하며, 연간 별도의 공공 예산을 받아야 한다. 또한 다른 감독기구와의 상호 지원 및 협력과 관련된 업무 등 효과적인 업무 수행에 필요한 재정·인적 자원, 부지, 기반 시설을 제공받을 수 있다(전문 제120항).

※ 감독기구의 독립성이 재정 지출이나 사법 심사와 관련된 통제 또는 모니터링의 대상으로부터 배제된다는 것을 의미하지는 않는다(전문 제118항).

### 선임 감독기구<sup>6)</sup>

다음에 해당하는 주 사업장 또는 단일 사업장을 관할하는 감독기구의 경우 선임 감독기구(Lead Supervisory Authority)가 된다.

- ① EU 내 컨트롤러나 프로세서의 사업장에서 개인정보 처리가 이루어지고 컨트롤러나 프로세서가 하나 이상의 회원국에 배치된 경우
- ② EU 내 설립된 컨트롤러나 프로세서의 단일 사업장에서 시행되는 정보 처리가 하나 이상의 회원국의 정보주체에 실질적으로 영향을 미치거나 미칠 가능성이 있는 경우(전문 제124항)

선임 감독기구는 정보주체가 자신의 개인정보 처리에 대하여 불만을 제기할 때, 국경을 초월하는 개인정보 처리 활동을 다룰 1차적 책임이 있다. 이 때 선임 감독기구는 다른 관련 있는 감독기구의 모든 조사에 협력하게 된다.

---

6) 제29조 작업반(2017. 4. 5.), Guidelines on the Lead Supervisory Authority, pp. 4-5.

## 더 알아보기 1

I  
개  
요

## 개인정보보호 법령과 GDPR의 주요 용어 비교

국내 개인정보보호 관련 법령과 EU의 GDPR은 일부 유사한 용어를 사용하는 것처럼 보이나 그 범위 및 역할 등이 상이한 용어가 존재합니다.

따라서 아래의 주요 용어에 명시한 개념의 차이를 이해하고 GDPR을 적용함에 있어 혼선이 없도록 해야 합니다.

한국(개인정보보호법)	EU(GDPR)	비고
민감정보(특별한 유형의 개인정보)		
[제23조제1항] 개인정보처리자는 <u>사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(유전자 검사 등의 결과로 얻어진 유전정보 및 '형의 실험 등에 관한 법률' 제2조제5호에 따른 범죄경력 자료에 해당하는 정보)</u> (이하 '민감정보'라 한다)를 처리해서는 아니된다.	[제9조] 컨트롤러는 인종·민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체 정보, 건강 정보, 성생활·성적 취향에 관한 정보를 처리해서는 안 된다. [제10조] 범죄경력 및 범죄행위에 관련된 개인정보의 처리 또는 제6조제1항에 근거한 관련 보안조치는 <u>공적권한의 통제 하에서 또는 그 처리가 정보주체의 권리 및 자유를 위한 적절한 안전장치를 규정하는 EU 또는 회원국 법이 허가하는 경우에만</u> 수행되어야 한다.	GDPR은 특별한 유형의 개인정보 (민감정보)와 범죄 경력 및 범죄행위에 관련한 개인정보를 구분하고, 그 처리 기준을 구분하였음
위탁자	컨트롤러	
[제26조제2항] 위탁자는 <u>개인 정보의 처리 업무를 위탁하는 개인 정보처리자를</u> 의미한다. 위탁자는 자신의 사무 처리를 위해 <u>통상 직접 수집한 개인정보</u> 를 수탁자에게 제공한다.	[제7조] 컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 주체를 의미한다. 컨트롤러는 <u>개인정보 처리의 목적과 수단을 규정하기만 하면</u> 족하며, 자신이 개인정보를 직접 수집하여 <u>프로세서에게</u> 제공할 필요는 없다.	GDPR의 컨트롤러는 처리의 목적과 수단을 규정하는 역할을 하며, 반드시 정보의 처리를 위탁할 필요는 없음
수탁자	프로세서	
[제26조제2항] 수탁자는 <u>위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자</u> 를 의미한다.	[제8조] 프로세서는 컨트롤러를 대신하여 <u>개인정보를 처리하는 개인, 법인, 정부부처 및 관련기관, 기타 단체 등을</u> 의미하며, 컨트롤러의 지시에 따라 개인정보를 처리한다.	

개인정보 보호 책임자	DPO
<p>[제31조제1항] 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호 책임자를 지정하여야 한다.</p> <p>[시행령 제32조제2항] 개인정보처리자는 법 제31조제2항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.</p> <p>1. 공공기관 : 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등</p> <p>2. 공공기관 외의 개인정보처리자 : 다음 각 목의 어느 하나에 해당하는 사람</p> <p>가. <u>기업주 또는 대표자</u></p> <p>나. <u>임원</u>(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)</p>	<p>[제37조제5항] DPO는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 제39조에 언급된 직무를 완수할 능력에 근거하여 지정되어야 한다.</p> <p>[제39조제1항] DPO는 최소한 다음의 직무를 가져야 한다.</p> <p>(a) <u>컨트롤러나 프로세서, 그리고 데이터 처리를 수행하는 해당 직원에게 GDPR과 EU 또는 회원국의 개인정보보호 조문에 따른 의무에 대하여 고지하고 조언</u></p> <p>(b) GDPR과 EU 또는 회원국의 개인정보보호 조문에 대한 컨트롤러 또는 프로세서의 <u>정책 준수 여부를 모니터링</u>(직원 교육과 감시 활동 포함)</p> <p>(c) 요청이 있을 경우, <u>개인정보보호 영향 평가에 관한 자료를 제공하고 평가 이행 상황을 감시</u></p> <p>(d) <u>감독기구와의 협력</u></p> <p>(e) 사전협의 등 처리에 관련된 사항에 대한 <u>감독기구의 연락처 역할</u>을 수행하며, 적절한 경우에는 <u>기타 사안에 대한 자료를 제공</u></p> <p>국내법 상 개인정보 보호책임자의 자격 요건은 공무원 또는 사업주, 대표자, 임원 등 일정 지위로 구분하나, GDPR 상 DPO는 전문적 자질, 특히 개인정보 보호법과 실무에 대한 전문적 지식 및 제39조에 언급된 직무를 완수할 능력에 근거하여 지정되어야 함</p>

## 더 알아보기 2

**가명처리(Pseudonymisation)****#1 가명처리**

GDPR은 정보주체의 위험을 감소시키고 컨트롤러와 프로세서의 의무를 충족시키는 보호조치 중 하나로서 가명처리(Pseudonymisation)를 제시하고 있습니다.

가명처리는 데이터 셋의 전체나 일부를 가상의 이름이나 부호로 대체함으로써 개인과의 연결성을 낮추는 데이터의 처리를 의미합니다. 즉 가명처리된 정보는 개인과의 연결이 깨지지 않은 정보로서 개인과의 연결이 깨진 익명처리 정보와 구분할 수 있습니다.

※ 다만 데이터의 익명처리 여부는 △연결 가능성, △추론 가능성, △싱글링 아웃 (Singling out) 여부를 모두 평가해야 함<sup>7)</sup>

다만 전문 제26항에서 GDPR은 가명처리된 정보는 추가적 정보를 이용하여 개인을 식별할 수 있는 정보이므로 식별 가능한 ‘개인정보’로 보아야 한다고 명시하고 있습니다<sup>8)</sup>.

**#2 가명처리의 활용**

가명처리는 개인정보를 처리할 때 위험성을 감소시키는 보호조치의 하나로, 정보주체가 갖는 위험성을 줄이고 컨트롤러와 프로세서의 개인정보보호 의무 준수를 위한 수단으로 활용할 수 있습니다.

그 예로 GDPR 제25조(Data Protection by Design and by Default)에서는 개인정보 처리 방법 결정 시점 및 처리 당시 시점에서 가명처리를 포함한 안전 조치를

7) Data Protection Commissioner, <https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm>.

8) 이와 관련하여 제29조 작업반은 가명화된 정보의 경우 개인 식별 가능성이 있으므로 데이터 보호를 위한 법적 체제의 범위 내에 두어야 한다는 의견을 밝히고 있다(제29조 작업반, Opinion 05/2014 on Anonymisation Techniques, p.10).



취해야 함을 규정합니다.

가명처리된 정보는 GDPR 준수 의무에서 완전히 배제되지 않지만 가명처리 기술을 사용하는 경우 컨트롤러에 대한 요구 사항이 완화되는 등의 인센티브를 기대할 수 있습니다.

GDPR 전문 제29항은 일반적인 분석을 허용하면서도, 특정 정보주체의 개인정보와 연결되는 추가적 정보를 별도로 보관할 수 있는 기술적·관리적 조치를 취할 때 가명처리를 통한 인센티브를 고려할 수 있다고 명시합니다.

### #3 가명화된 정보의 활용

GDPR은 제6조제4항을 통하여 개인정보 처리의 당초 목적과 양립 가능성 여부를 판단하는 보호조치 중 하나로 가명조치를 지목하고 있습니다.

특히 전문 제50항 및 제156항은 공익을 위한 기록 보존의 목적, 과학이나 역사적 연구의 목적, 또는 통계 목적인 경우의 정보 처리는 당초 목적과 양립 가능성이 있는 것으로 보고 가명처리를 통하여 추가적인 개인정보 처리가 가능하다고 밝히고 있습니다. 다만 추가적 정보는 제4조제5항에 따라 기술적·관리적 조치 하에 별도 분리 보관되어야 하며, 이 경우 재식별은 엄격히 금지됩니다.





## II. GDPR 인식 제고와 준비

---

1. 제정 목적과 법적 성격
2. GDPR의 구성 체계
3. 적용 대상과 범위

# 1

## 제정 목적과 법적 성격

### Point

- Directive에 비해 변화된 GDPR의 차이점을 설명할 수 있다.
- GDPR 시행이 우리 기업에 미치는 영향을 알 수 있다.

### 1.1 제정 목적과 의의

GDPR은 자연인에 관한 기본권과 자유(특히 개인정보보호에 대한 권리)를 보호하고(제1조제2항), EU 역내에서 개인정보의 자유로운 이동(제1조제3항)을 보장하는 것을 목적으로 한다.

또한 GDPR은 개인정보 삭제권, 처리 제한권, 개인정보 이동권, 반대권 등의 신규 권리 추가 및 기존 권리 명확화를 통하여 기존 Directive보다 정보주체의 권리를 확대·강화하였으며, DPO의 지정, Data protection by design and by default 등의 내용을 통하여 기업의 책임성을 강화하였다.

### 1.2 법적 효력

GDPR은 종래의 지침(Directive)이 아니라 Regulation이라는 법 형식으로 규율되어 법적 구속력을 가지며, 모든 EU 회원국에게 직접적으로 적용된다(제99조).

기존 Directive에서는 회원국 간 개인정보보호 법제가 서로 달라 규제에 어려움이

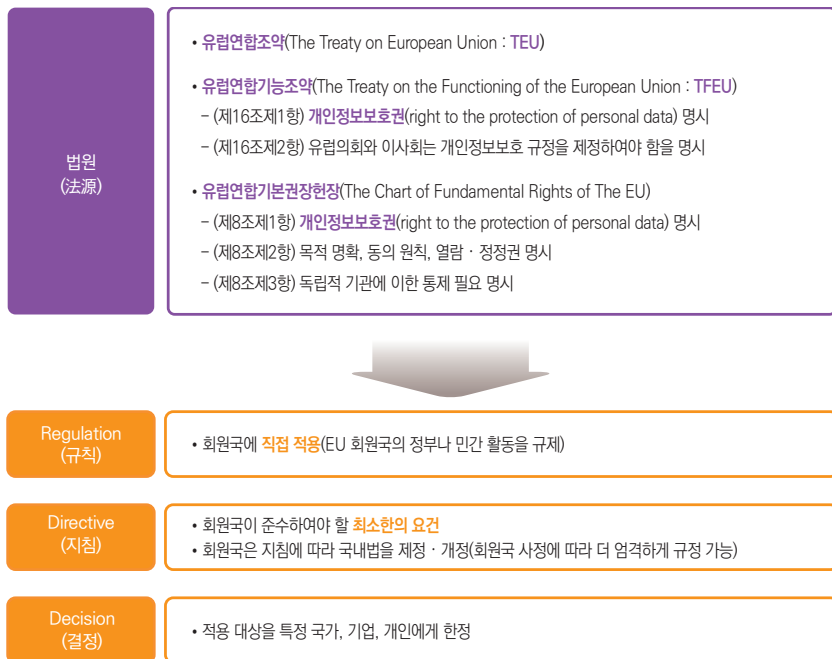
있었으나, GDPR 제정을 통하여 보다 강력하고 통일된 개인정보보호 규제가 가능하게 되었다.

※ Directive는 각 회원국에 대한 입법 지침 가이드라인 역할을 할 뿐이므로, 지침을 반영한 각국의 개별 입법이 필요하다.

그러나 GDPR 일부 규정에 대해서는 회원국의 별도 입법이 요구되므로, 기업들은 GDPR 이외에 각 회원국의 개인정보보호 관련 입법 동향에 대하여 지속적으로 모니터링할 필요가 있다.

※ 그 동안 시행되어 온 Directive 95/46/EC는 GDPR(2018. 5. 25. 시행과 동시)로 대체 되었다.

[그림 1] EU의 법 체계



### 1.3 GDPR 시행이 미치는 영향

기존 Directive는 처리되는 개인정보의 정보주체가 다수의 국가에 흩어져 있는 경우 단일의 감독기구를 통하는 것에 대한 규정이 별도로 명시되어 있지 않았다.

또한 컨트롤러는 법적 구속력이 없는 Directive와 함께 EU 회원국들 간 서로 다른 별도의 법제를 준수해야 했으므로 과도한 규제 체계로 인한 비용이 가중되어 왔다.

GDPR에서는 one-stop-shop 메커니즘의 도입과 법적 구속력 있는 단일한 규칙을 적용함으로써 기업이 사업 수행에 따르는 필요 비용을 절약할 수 있도록 하였다.

EU에서는 이로 인해 역내 시장의 진입 장벽이 낮아져 시장 기능이 크게 활성화될 것으로 예상하고 있으며, 디지털 단일 시장 조성 등 사업 규제 환경 개선으로 2020년 까지 7,390억 유로의 경제 효과를 기대하고 있다.<sup>9)</sup>

#### GDPR 관련 규정

- 제94조(Directive 95/46/EC의 폐기)
- 제99조(시행과 적용)

#### 셀프 체크리스트

- |   |                               |                                 |
|---|-------------------------------|---------------------------------|
| • GDPR 시행에 따라 영향을 받는 자사의 비즈니스를 파악하고 있다.                       | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
| • 사업장이 위치하고 있는 회원국과, 해당 회원국에서 준수해야 하는 법률(근로법 등)의 내용을 식별하고 있다. | <input type="checkbox"/>      | <input type="checkbox"/>        |

9) European Data Market Study SMART 2013/0063, <http://datalandscape.eu/>

## 2

# GDPR의 구성 체계

GDPR은 전문 총 173개항, 본문 총 11장 99개 조항으로 이루어져 있으며, 기존 Directive가 총 7장 34개 조항으로 구성된 것에 비해 조문 수가 크게 증가하였다.

[표 3] GDPR의 구성 체계

전문(Recital) 173항	
본문 11장(Chapter) 99개 조항(Article)	제1장 일반 규정(General Provisions)
	제2장 원칙(Principles)
	제3장 정보주체의 권리(Rights of the Data Subject)
	제4장 컨트롤러와 프로세서(Controller and Processor)
	제5장 제3국 및 국제기구로의 개인정보 이전 (Transfer of Personal Data to Third Countries or International Organizations)
	제6장 독립적인 감독기구(Independent Supervisory Authorities)
	제7장 협력과 일관성(Cooperation and Consistency)
	제8장 구제책, 책임, 벌칙(Remedies, Liability and Penalties)
	제9장 특정 정보 처리 상황에 관한 규정 (Provisions Relating to Specific Data Processing Situations)
	제10장 위임 입법 및 이행 입법(Delegated Acts and Implementing Acts)
	제11장 최종 규정(Final Provisions)



## 3 적용 대상과 범위

### Point

- GDPR의 적용을 받는 정보를 구분할 수 있다.
- GDPR이 적용되는 물적 범위와 지리적 범위를 이해할 수 있다.

### 3.1 적용 대상(제1조)

#### 3.1.1 어떤 정보에 적용되는지

GDPR은 개인정보 처리에 대하여 적용된다. GDPR은 판례 및 개별법 등을 통해 표명되어 온 개인정보의 개념을 조문에 포함함으로써 적용 대상을 보다 구체적으로 명시하고 있다.

특히 개인과의 연결성이 있는 가명처리된 정보를 개인정보로 명시함으로써 GDPR의 적용범위 안에 두었다(전문 제26항).

또한 GDPR은 '민감정보(Special categories of personal data)'를 규정하고 있는데, 이는 인종·민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부, 유전자 또는 생체 정보, 건강, 성생활 또는 성적 취향에 관한 정보를 포함한다. 민감정보는 정보주체의 명시적 동의 획득 등의 경우를 제외하고는 원칙적으로 처리가 금지된다.

#### 3.1.2 누구에게 적용되는지

GDPR은 정보주체인 '살아 있는 자연인'의 개인정보에 국한되며, 국적이나 거주지에

관계 없이 본인의 개인정보 처리에 관련된 ‘개인’에 적용된다. 다만 사망한 사람의 개인정보 처리와 관련하여 개별 회원국이 별도 조항을 두는 것을 제한하지 않는다.

GDPR은 법인과 법인으로 설립된 사업체 이름, 법인 형태, 법인 연락처 등에 대한 처리에는 적용되지 않는다(전문 제14항).

## 3.2 적용 범위

### 3.2.1 물적 범위(Material scope)(제2조제1항)

GDPR은 전체 또는 부분적으로 자동화된 수단에 의한 개인정보의 처리에 적용된다(전자적 데이터베이스나 컴퓨터로 운영되는 파일링 시스템 등).

다만 수기 처리(manual processing)와 같이 비자동화 수단에 의한 개인정보 처리라고 하더라도 (관련성 있는) 파일링 시스템의 일부를 구성하는 경우 등에는 적용 대상이 된다.

### 3.2.2 지리적 범위(Territorial scope)(제3조)

〈EU 역내: EU에 사업장을 운영하며, 해당 사업장이 개인정보 처리를 수반하는 경우〉

컨트롤러 또는 프로세서가 EU에 사업장(establishment)을 가지고 있고, 해당 사업장에서의 활동이 개인정보의 처리를 포함한다면 GDPR이 적용된다.

‘사업장’이 무엇을 의미하는지는 GDPR에 구체적으로 정의되어 있지 않다. 다만 사업장은 일정한 조치(stable arrangements)를 통하여 효과적이고 실질적(effective and real exercise of activity) 활동을 수행하는 경우를 의미한다.

이러한 사업장의 범위는 자회사(subsidiary)뿐만 아니라 지사(branch)를 포함할 수 있다.

〈EU 역외: EU에 있는 정보주체에게 재화나 서비스를 제공 하는 경우 또는 EU 내 정보주체의 행동에 대한 모니터링〉

EU에 사업장을 가지고 있지 않더라도 다음에 해당하는 경우에는 GDPR이 적용된다.

- ① EU 내에 있는 정보주체에게 재화나 서비스를 제공(offering)하는 경우
  - ※ 정보주체가 실제로 재화 또는 서비스의 비용을 지불하였는지 여부와는 무관하다.
- ② EU 내에 있는 정보주체에 대하여 EU 내에서의 행동을 모니터링하는 경우

### 3.3 적용 예외(National derogations)(제2조제2항)

GDPR은 다음 경우에 해당하는 개인정보 처리에는 적용되지 않는다.

- ① EU 법률의 범위를 벗어나는 활동
  - ※ EU 개별 회원국의 형사법과 관련하여 수행되는 활동
- ② 개별 회원국에서 수행하는 EU의 공동 외교 안보 정책과 관련된 활동
- ③ 자연인이 순수하게 수행하는 개인 또는 가사 활동(purely personal or household activities)
- ④ 공공 안전의 위협에 대한 보호 및 예방을 포함하여, 관할 감독기구(competent authorities)의 범죄 예방, 수사, 탐지, 기소 및 형사 처벌 집행 관련 활동

#### GDPR 관련 규정

- 제1조(대상 및 목적)
- 제2조(물적 범위)
- 제3조(지리적 범위)

#### 개인정보보호법 관련 규정

- 제2조(정의)

### 셀프 체크리스트

- |   | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
|---|-------------------------------|---------------------------------|
| • 처리하고 있는 개인정보의 유형이 GDPR의 적용을 받는지 여부를 알고 있다.                  | <input type="checkbox"/>      | <input type="checkbox"/>        |
| • 개인정보 처리 수단이 자동화된 수단이나 파일링 시스템을 구성하는 수기 처리에 해당하는지 여부를 알고 있다. | <input type="checkbox"/>      | <input type="checkbox"/>        |
| • 개인정보 처리가 EU 역내 혹은 역외에서 어떤 목적과 형태로 이뤄지는지 식별하고 있다.            | <input type="checkbox"/>      | <input type="checkbox"/>        |



## Ⅲ. 주요 원칙

---

1. 개인정보 처리 원칙(Principles)
2. 처리의 적법성(Lawfulness of processing)
3. 동의(Consent)
4. 아동 개인정보(Children's personal data)
5. 민감정보 및 범죄행위 관련 정보(Special categories of personal data  
& Personal data relating to criminal convictions and offences)

# 1

## 개인정보 처리 원칙 (Principles)

### (제5조)

#### Point

- 개인정보를 처리할 때 준수하여야 하는 7가지 기본 원칙을 이해할 수 있다.

#### 1.1 적법성·공정성·투명성의 원칙(Lawfulness, fairness and transparency)

정보주체의 개인정보는 적법하고 공정하며 투명한 방식으로 처리되어야 한다.

여기에서 투명성은 개인정보를 처리하는 일련의 행위에서 정보주체에게 이해하기 용이하고, 접근하기 쉬운 공개된 방식으로 처리 행위를 입증하는 것을 뜻한다.

#### 1.2 목적 제한의 원칙(Purpose limitation)

구체적·명시적이며 적법한 목적을 위하여 개인정보를 수집하여야 하며, 해당 목적과 부합하지 않는 방식의 추가 처리는 허용되지 않는다.

다만 공익을 위한 기록 보존 목적, 과학적·역사적 연구 목적, 또는 통계 목적을 위한 추가 처리는 해당 목적과 양립하는 것으로 본다.

### 1.3 개인정보 처리의 최소화(Data minimisation)

개인정보의 처리는 적절하며 관련성이 있고, 그 처리 목적을 위하여 필요한 범위로 한정되어야 한다.

### 1.4 정확성의 원칙(Accuracy)

개인정보의 처리는 정확하여야 하며, 필요 시 처리되는 정보는 최신으로 유지되어야 한다. 따라서 처리 목적에 비추어 부정확한 정보의 즉각적인 삭제 또는 정정을 보장하기 위한 모든 합리적 조치가 취해져야 한다.

### 1.5 보유 기간 제한의 원칙(Storage limitation)

개인정보는 처리 목적상 필요한 경우에 한하여 정보주체를 식별할 수 있는 형태로 보유되어야 한다.

정보주체를 식별할 수 있는 개인정보는 처리 목적상 필요한 경우에 한하여 보유되어야 한다.

### 1.6 무결성과 기밀성의 원칙(Integrity and confidentiality)

개인정보는 적절한 기술적·관리적 조치를 통하여 권한 없는 처리, 불법적 처리 및 우발적 손·망실, 파괴 또는 손상에 대비한 보호 등 적절한 보안을 보장하는 방식으로 처리되어야 한다.



1.7 책임성의 원칙(Accountability)

컨트롤러는 위의 원칙을 준수할 책임을 지며, 이를 입증할 수 있어야 한다.

GDPR 관련 규정

- 제5조(개인정보 처리 관련 원칙)

개인정보보호법 관련 규정

- 제3조(개인정보보호 원칙)

셀프 체크리스트

	예	아니오
• 개인정보 처리 목적에 필요한 최소한의 개인정보만을 수집하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 법적 요건 등 처리 목적을 달성하거나 보유 기간이 만료된 경우 가능한 한 신속하게 개인정보를 파기하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 기술적·관리적 조치를 통하여 적절한 개인정보 보호조치를 수행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

## 2

# 처리의 적법성

## (Lawfulness of processing)

### (제6조)

#### Point

- 개인정보의 적법한 처리 근거를 이해할 수 있다.

GDPR에 따른 적법한 처리가 되려면, 기업은 개인정보 처리 전에 법적 근거(이하 ‘적법한 처리 조건’)를 확인하여야 한다.

다음 각 호는 개인정보 처리를 위하여 적용 가능한 적법 처리 근거를 명시하고 있다 (제6조제1항).

- ① 정보주체가 하나 이상의 특정한 목적을 위하여 개인정보 처리에 동의한 경우(a)
- ② 정보주체가 당사자인 계약의 이행을 위하여 또는 계약 전 정보주체 요청에 응하기 위한 처리(b)
- ③ 컨트롤러에게 적용되는 법적 의무 이행을 위하여 필요한 처리(c)
- ④ 정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위하여 필요한 처리(d)
- ⑤ 공익을 위하여 수행되는 직무의 이행 또는 컨트롤러에게 부여된 공적 권한의 행사에 필요한 처리(e)
- ⑥ 컨트롤러 또는 제3자의 적법한 이익 추구 목적을 위하여 필요한 경우로써, 정보주체가 아동인 경우와 같이 정보주체의 이익과 권리 또는 자유가 그 이익보다 중요한 경우는 제외(f)

※ 다만 이 조건은 정부부처가 그 임무 수행을 위하여 처리한 경우에는 적용되지 않는다.

이 때, GDPR은 회원국들이 법적 의무 이행을 위하여 필요한 처리[제6조제1항(c)] 및 공익을 위한 임무 수행 또는 컨트롤러의 공적 권한의 행사를 위하여 필요한 처리[(e)]에 관련하여 보다 구체적으로 규정하는 것을 허용하고 있다.

**GDPR 관련 규정**

- 제6조(처리의 적법성)

**셀프 체크리스트**

- 개인정보를 처리할 때 GDPR과 해당 국가의 관련 법적 근거를 반영하여 처리하고 있다.

예  
☐

아니오  
☐

# 3

## 동의

### (Consent)

#### (제7조)

#### Point

- Directive보다 강화된 GDPR의 동의 조건을 이해할 수 있다.
- 명시적 동의가 필요한 경우와 그 획득 방법을 알 수 있다.

### 3.1 동의의 정의

GDPR에서 동의는 정보주체가 진술 또는 적극적 행동을 통하여 자신의 개인정보 처리에 대한 긍정적 의사를 표현하는 것을 의미한다.

이 때 정보주체의 동의는 '진정한(genuine)' 것이어야 하며, 이는 형식적인 요건의 충족만으로 달성할 수 없다. 특히 강제, 압박, 자유 의지 행사의 제한 등과 같은 요소가 존재하는 경우의 동의는 자유롭게 제공한 것이 아니며, 유효한 동의가 될 수 없다.

Directive와 GDPR 간 동의에 대한 정의는 유사하지만 GDPR은 동의 방법에 구체성이 필요함을 명시하였으며, 즉 '표시가 모호하지 않아야 하고, 명확하고 적극적인 행위'가 따라야 한다는 점을 추가하였다.

## 3.2 동의의 유효 조건(Valid consent)

### 3.2.1 자유롭게 부여된 동의(Free / Freely given)<sup>10)</sup>

동의란 정보주체에게 본인의 개인정보 처리에 대하여 실질적인 선택권과 통제권을 부여하는 것을 의미한다. 정보주체가 반드시 동의하여야 한다고 강제적인 느낌을 받는 등 개인에게 실질적 선택권이 없다면 유효한 동의로 보지 않는다.

따라서 동의의 거부에 따른 불이익이 없어야 하며, 언제든지 동의를 쉽게 철회할 수 있어야 한다.

- ① 동의가 자유롭게 제공되도록 보장하기 위하여 정보주체와 컨트롤러 사이에 명백한 불균형이 있는 특정 상황의 경우에는 동의를 개인정보 처리에 유효한 법적 근거로 볼 수 없다. 이 때 개인정보 처리에 대한 동의 문구를 일반적인 '이용 약관(general terms and conditions)'에 포함하여 제시하여서는 안 된다(제7조제4항<sup>11)</sup>, 전문 제43항<sup>12)</sup>).

#### 참고·예시

서비스를 이용하기 위해서는 GPS 기능을 작동하도록 요구하는 사진 편집 모바일 앱이 있다. 해당 앱은 수집한 정보를 행태 광고의 목적으로 활용할 것이라고 안내하였다. 이 때 GPS 기능의 작동이나 행태 광고의 제공은 해당 모바일 앱 서비스를 제공하기 위하여 필수적인 것은 아닐 수 있다. 이용자가 필수적이지 않은 목적에 동의하지 않아 해당 앱을 이용할 수 없는 경우라면, 이러한 상황에서의 동의는 자유롭게 제공한 것이 아닌 것으로 본다.

- ② 컨트롤러는 정보주체가 불이익 없이(without detriment) 동의를 거부 또는 철회할 수 있다는 것을 입증하여야 한다. 예를 들어 동의의 철회에 따른 비용이 발생하지

10) 제29조 작업반(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp. 5-10.

11) '동의를 자유롭게 부여되는지를 평가할 때, 서비스 제공을 포함한 계약 이행이 그 계약의 이행에 필요하지 않은 개인 정보 처리에 대한 동의를 조건으로 하지 않는지 세심하게 살펴야 한다.'

12) '서비스 제공을 포함한 계약 이행에 동의가 필요하지 않음에도 불구하고 동의에 의존하는 경우, 동의가 자유로이 부여되지 않는 것으로 본다.'

않는다거나, 동의 철회에 대하여 강압이나 기망 등 중대한 부정적 결과가 발생하지 않는다는 것을 입증할 수 있는 경우 동의가 자유롭게 제시되었음을 입증하는 데에 도움이 될 수 있다.

### 3.2.2 개별적으로 특정한 동의(Specific)<sup>13)</sup>

정보주체의 이용자 통제권 및 투명성을 확보하기 위하여 동의의 내용은 개별적으로 특정되어야 한다. 개별적으로 특정한 동의의 요건을 충족하기 위하여 컨트롤러는 다음 사항을 적용하여야 한다.

- ① 기능 확대(function creep) 현상<sup>14)</sup>에 대비한 안전 조치로서의 목적 명확화
  - 개인정보 처리의 목적을 사전에 명확하게 규정하지 않는 경우, 개인정보 처리의 목적이 점진적으로 확대되거나 불명확해지는 기능 확대 현상이 발생할 수 있다. 이는 정보주체가 예상할 수 없는 개인정보 처리를 발생시켜 통제권을 상실시키므로 개인정보 처리에 위험을 발생시킬 수 있다.
- ② 동의 메커니즘의 상세화
  - 동의 메커니즘이 상세해야 한다는 것(be granular)은 컨트롤러가 여러 다른 개별 목적에 대한 개별적 옵트인(opt-in)을 제공해야 함을 의미한다. 즉 정보주체는 특정 목적에 대하여 해당하는 특정 동의를 제공할 수 있어야 한다.

#### 참고·예시

도매상이 마케팅 목적으로 이메일을 발송하기 위하여 개인정보를 이용하는 것과 그룹사에서 고객 개인정보를 공유하기 위하여 개인정보를 사용하는 것 등 두 가지 목적에 대하여 한 가지 동의 요청서를 제시한 경우, 그 동의 요청서는 두 가지 개별적 개인정보 처리 목적에 대하여 하나의 동의만을 제시한 것으로, 세부적인 것으로 볼 수 없다. 따라서 이러한 경우의 동의는 유효한 것으로 볼 수 없다.

13) 제29조 작업본(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp. 11~12.

14) 기능 확대(function creep) 현상: 프로젝트가 시작한 시점 이후 프로젝트의 범위가 지속적으로 또는 통제되지 않은 채 확대되는 현상.

③ 동의 획득과 관련한 정보와 다른 정보의 명확한 분리

- 컨트롤러는 서로 다른 목적을 지닌 각각의 동의 항목에 따라 개별적으로 특정한 정보를 제공하여야 한다. 이렇게 함으로써 정보주체는 자기의 선택이 가져오는 결과나 영향에 대하여 인식할 수 있다.

3.2.3 사전 정보가 제공된 동의(Informed)<sup>15)</sup>

GDPR은 동의 조건으로 정보주체에게 동의에 대한 정보를 제공하는 것(requirement that consent must be informed)을 강조하고 있다.

정보주체에게 동의에 대한 사전 정보를 제공하는 것은 정보주체의 의사결정에 도움을 준다. 즉 정보주체가 그들이 동의하는 것이 어떤 의미가 있으며, 어떤 영향을 미칠 것인지 이해하도록 하여 정보주체의 권리 행사(예: 동의의 철회 등)를 가능하게 한다.

정보주체가 '사전 정보가 제공된' 동의를 할 수 있도록 컨트롤러는 정보주체의 선택을 도울 수 있는 핵심 요소를 알려 줄 필요가 있다. 핵심 요소는 최소한 다음 사항을 포함하여야 한다.

- ① 컨트롤러의 신원
- ② 동의를 구하는 개별 처리 활동의 목적
- ③ 수집 및 이용되는 개인정보 또는 개인정보의 유형
- ④ 동의 철회권의 존재
- ⑤ 제22조제2항에 따른 프로파일링 등 자동화된 개인정보 처리를 바탕으로 한 결정에 사용되는 개인정보에 대한 정보
- ⑥ (개인정보 이전에 대한 동의인 경우) 적정성 결정 및 적절한 보호조치가 존재하지 않는 제3국으로의 개인정보 전송에 따라 발생 가능한 위험에 대한 정보 [제49조 제1항(a)]

15) 제29조 작업반(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp. 12~14.

다만 이 중 ① 또는 ⑥에 대한 정보는 개인정보보호처리방침(Privacy Policy)에 포함되어 제시될 수 있다.

GDPR은 동의에 필요한 정보를 제공하는 ‘방식’에 대해서는 특별한 규정을 두고 있지 않으나, 동의(문구)는 일반인이 이해할 수 있고, 누구나 쉽게 접근 가능한 형태로 제시되어야 하며, 다른 사안들과 명확히 구분되어야 한다.

### 3.2.4 정보주체의 명확한 의사 표시(Unambiguous indication)<sup>16)</sup>

동의를 반드시 개인정보 처리 활동이 발생하기 전에 획득되어야 하며(opt-in), 정보주체가 동의하였다는 사실과 동의한 내용이 분명하여야 한다. 이를 위해서는 동의 조건을 읽었음을 확인하는 것만으로는 부족하며, 전자적 수단을 포함한 서면진술(또는 구두진술)과 같은 명확한 긍정 행위(clear affirmative act)가 있어야 한다(전문 제32항).

‘명확한 긍정 행위’란 특정한 처리 행위에 대하여 동의를 ‘의식적 행동’으로 표시하는 것을 의미하며, 다음 경우에는 동의를 위한 명확한 표시로 인정될 수 없다.

- ① 사전에 선택되어 있는 체크박스(pre-ticked boxes)를 제시하는 것
- ② 암묵적(silence) 동의나 부작위(inactivity)를 동의로 보는 것
- ③ 서비스가 제시하는 절차를 동의 의사 표시 없이 단순히 진행하는 것
- ④ 일반적 이용 약관에 포괄적 수용(이른바 ‘blanket acceptance’) 의사를 표현한 것

‘서면진술’의 방법은 정보주체가 편지나 이메일을 통하여 컨트롤러에게 동의 의사를 표시하는 방법 등을 포함하는데, 현실적으로 GDPR의 준수 범위에서 여러 가지 형태와 크기로 이루어질 수 있다.

‘전자적 수단’에 따라 동의가 주어지는 경우 동의 요청이 서비스 이용에 불필요한 지장을 주어서는 안 된다. 다만 동의가 정보주체의 적극적·긍정적 동작(active

16) 제29조 작업반(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp. 15~17.



affirmative motion)으로 효력을 갖기 위하여 서비스 이용에 어느 정도 지장을 주는 것은 불가피할 수 있다.

#### 참고·예시

- 스크린을 넘기고(swiping), 스마트폰 카메라 앞에서 손을 흔들고(waiving), 스마트폰을 쥐어 시계 방향으로 돌리고(rotating), 스마트폰을 들어 공중에 8자 모양을 그리는 등의 방식으로 동의를 명확히 표시하도록 할 수 있다. 다만 이와 같은 경우에도 명확한 동의 문구가 제시되어야 하며, 이와 같은 방식으로 동의를 받았음을 컨트롤러가 사후 입증할 수 있어야 한다. 아울러 동의 취소 방식이 동의 획득 방식과 동일한 수준으로 용이하여야 한다.
- 위와 같은 방식이 허용됨에도 불구하고, 동의 문구를 포함하는 이용 약관을 화면에 노출하여 이용자가 이를 연속적으로 내리거나 스크린을 넘기도록(scrolling down or swiping) 하는 것은 동의의 명확성 요건을 충족하지 못하는 것으로 이해된다. 이처럼 많은 약관 내용이 연속적으로 노출될 경우 정보주체가 동의 문구를 열람하지 못한 채 화면의 하단까지 이르게 될 수 있기 때문에 충분히 명확한 것으로 볼 수 없다.

### 3.3 명시적 동의(Explicit consent)가 필요한 경우<sup>17)</sup>

GDPR은 중대한 개인정보보호 위험이 발생하여 정보주체에게 개인정보에 대한 높은 수준의 통제권이 필요하다고 보는 경우 정보주체의 명시적(explicit) 동의를 요구하고 있다.

‘명시적’의 개념은 정보주체가 동의를 표현하는 방식을 의미하여, 정보주체가 명확한 의사 표시를 해야 함을 의미한다. 구체적인 방법으로는 서면진술, 동의 의사가 표명된 이메일 발송, 정보주체의 서명이 포함된 스캔 문서의 업로드, 전자 서명 요구, 동의에 대한 2단계 검증 등이 있다.

17) 제29조 작업반(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp.18-20.

## 참고·예시

- [동의에 대한 2단계 검증] (1단계) 정보주체는 의료 정보가 포함된 기록을 처리하고자 하는 컨트롤러의 통지 이메일을 수신한다. 이메일에서 컨트롤러는 특정 목적을 위하여 특정 정보를 사용하는 데 대한 동의를 요구한다는 것을 설명한다. 컨트롤러는 정보주체가 이 정보의 사용에 동의할 경우 '동의합니다(I agree)'라는 진술이 포함된 이메일을 회신할 것을 요구한다.  
(2단계) 회신 후 정보주체는 반드시 클릭해야 하는 확인 링크 또는 동의를 확인하는 확인 코드가 포함된 SMS 메시지를 수신한다.
- 웹사이트 운영자가 사이트 방문자에게 '나는, ○○ 웹사이트가 나의 개인정보를 처리하는 것에 동의합니다.(I, hereby, consent to the processing of my data)'라는 문구와 함께 'Yes ☐ / No ☐의 체크박스를 제공하고 이에 대하여 이용자로 하여금 체크하도록 하여 명시적 동의를 받을 수 있다. 다만 이 경우 사전에 정보가 제공된 동의 요건 및 기타 '유효한 동의(valid consent)'에 필요한 요건을 모두 충족하여야 한다.

GDPR은 다음 조항에 해당하는 경우 명시적 동의가 필요함을 명시하고 있다.

- ① 민감정보의 처리(제9조)
- ② 역외 이전 시 특정 상황에 대한 예외 조항(제49조)
- ③ 프로파일링을 포함한 자동화된 의사결정(제22조) 등

### 3.4 동의를 철회(Withdrawal of consent)<sup>18)</sup>

동의를 철회는 GDPR에서 정보주체의 권리 행사에 중요한 위치를 차지하며, 컨트롤러는 정보주체가 동의를 제공할 때와 마찬가지로 언제든지 철회할 수 있도록 보장하여야 한다고 규정하고 있다(제7조제3항).

GDPR은 동의를 철회 행위가 동의를 제공 행위와 반드시 동일해야 한다고 설명하지 않는다. 다만 한 번의 마우스 클릭이나 스와이프, 또는 키 누름 등의 전자적 수단으로 쉽게 동의를 획득하는 경우, 동의를 철회도 마찬가지로 쉽게 이루어질 수 있어야 한다.

18) 제29조 작업반(2018. 4. 16.), Guidelines on Consent under Regulation 2016/679, pp. 21~23.

### 참고·예시

- 온라인 대행사를 통하여 티켓을 판매하는 음악회가 있다. (동의 수단) 컨트롤러는 티켓을 판매할 때마다 연락처 세부 정보를 마케팅 목적으로 사용하기 위하여 예·아니오 형식으로 동의를 요구한다. (철회 수단) 반면 컨트롤러는 고객에게 영업일 오전 8시부터 오후 5시 사이 콜센터에 무료 연락을 통하여 동의를 철회할 수 있다는 것을 고지한다.
- 이 사례에서 컨트롤러는 GDPR 제7조제3항을 준수하지 않은 것으로 본다. 이 경우 동의를 철회하려면 영업 시간 중에 전화를 걸어야 하는데, 이는 휴일 없이 24시간 열려 있는 온라인 티켓 대행사를 통하여 동의하는 데 필요한 한 번의 마우스 클릭보다 더 번거롭기 때문이다.

### GDPR 관련 규정

- 제4조(정의) 제11항
- 제7조(동의의 조건)
- 제22조(프로파일링을 포함한 자동화된 의사결정)
- 제49조(특정 상황에 대한 역외 이전 예외 조항)
- 전문 제32항, 제42항, 제43항

### 개인정보보호법 관련 규정

- 제4조(정보주체의 권리) 제2호
- 제15조(개인정보의 수집·이용)
- 제16조(개인정보의 수집 제한)
- 제17조(개인정보의 제공)
- 제18조(개인정보의 목적 외 이용·제공 제한)
- 제19조(개인정보를 제공받은 자의 이용·제공 제한)
- 제22조(동의를 받는 방법)

### 셀프 체크리스트

	예	아니오
• 개인정보 처리가 정보주체의 동의에 근거하는 경우, 법적 요건을 준수하여 유효한 동의를 받고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리가 정보주체의 동의에 근거하는 경우, 동의 획득 대상에 대하여 누락 없이 동의를 받고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 민감정보 처리 등 정보주체에게 개인정보에 대한 높은 수준의 통제권이 필요하다고 보는 경우, 동의 의사가 들어간 이메일, 서명 등을 통해 정보주체의 명시적 동의를 받고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 개인정보 처리에 동의하였음을 입증할 수 있도록 동의에 대하여 기록 및 보관하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 쉽게 동의를 철회할 수 있도록 적용되어 있다.	<input type="checkbox"/>	<input type="checkbox"/>

## 4

## 아동 개인정보 (Children's personal data) (제8조)

## Point

- '아동'에 대한 개인정보 보호조치 강화 기준을 이해할 수 있다.
- 아동 개인정보를 처리할 때 준수하여야 하는 개인정보 처리 규정을 이해할 수 있다.

### 4.1 아동에 대한 특별한 보호 필요성

GDPR은 아동의 경우 개인정보 처리에 따른 위험성과 그 결과 그리고 본인의 권리를 잘 인지하지 못할 수 있으므로 개인정보와 관련하여 특별한 보호가 필요함을 명시하고 있다(전문 제38항).

따라서 GDPR은 아동의 동의 관련 규정(제8조) 외에도 법 전반에 걸쳐 아동에 관한 개인정보보호를 강조하고 있다[제6조제1항(f), 제57조제1항(b), 제40조제2항(g) 및 전문 제38항, 제58항, 제65항, 제71항].

### 4.2 아동에게 제공되는 온라인 서비스 및 친권자 동의

만 16세 미만의 '아동에게 직접' 정보사회서비스(information society services)를 제공할 때 부모 등 친권을 보유하는 자(holder of parental responsibility)의 동의를 받도록 요구하고 있다.

※ 다만 정보사회서비스 제공자가 잠재적 고객에게 해당 서비스가 성인에게만 제공되는 것을 명확히 하고, 이러한 사실이 사이트의 콘텐츠나 마케팅 계획 등 다른 요소에도 위배되지 않는 경우 해당 서비스는 '아동에게 직접' 제공되는 것이 아닌 것으로 판단된다.

그러나 각 회원국은 자국의 법률을 통하여 친권자 동의를 요하는 아동의 연령 기준을 만 13세 미만까지 낮추어 규정할 수 있다.

[표 4] EU 회원국의 친권자 동의가 필요한 아동 연령<sup>19)</sup>

기준 연령	해당 국가
만 13세	덴마크, 라트비아, 벨기에, 스웨덴, 스페인, 아일랜드, 에스토니아, 영국, 포르투갈, 폴란드, 핀란드
만 14세	불가리아, 오스트리아, 이탈리아, 키프로스
만 15세	그리스, 슬로베니아, 체코
만 16세	네덜란드, 독일, 루마니아, 룩셈부르크, 리투아니아, 몰타, 슬로바키아, 크로아티아, 프랑스, 헝가리 * 프랑스는 개인정보보호에 관한 법안(Draft Bill on the Protection of Personal Data) 제59조에 따라 건강에 관련한 조사, 연구 또는 평가의 경우 만 15세(또는 그 이상)으로 규정하고 있다.

※ 위 내용은 잠정적 현황(provisional indications)이므로 이후 변동될 수 있음

동의를 바탕으로 아동에게 정보사회서비스를 제공하는 경우, 컨트롤러는 아동의 연령이 디지털 동의 기준 연령보다 높은지 검증하기 위한 ‘합리적 노력’을 하여야 한다. 이와 같은 노력 수준은 개인정보 처리 활동의 성격과 위험에 비례하여야 한다. 비록 GDPR은 연령 검증의 필요성을 명시적으로 요구하지는 않으나, 동의 연령에 도달하지 않은 아동의 동의를 기반으로 한 개인정보 처리는 적법하지 않다.

동의를 제공하는 자가 동의를 표시할 수 있는 연령에 도달하였는지, 그리고 동의를 제공하는 자가 아동에 대한 부모의 책임을 보유한 자인지를 합리적으로 확인하는

19) betterinternetforkids(2018. 5. 5.), <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751>.

방식은 개인정보 처리에 내재된 위험과 가용한 기술에 따라 다르다.

- ① 위험이 낮은 수준인 경우, 이메일을 이용하여 부모로서의 책임이 존재하는지 검증하는 것만으로 충분하다.
- ② 위험이 높은 수준인 경우, 컨트롤러가 제7조제1항에 따라 정보주체의 동의를 입증할 수 있는 정보를 확인하고 보유할 수 있도록 더 많은 증거를 요구할 수 있다.

#### 참고·예시

- 한 온라인 게임 플랫폼은 부모나 보호자의 동의가 있는 경우에만 아동에게 게임 서비스를 제공하려고 한다. 이 경우 컨트롤러는 다음과 같은 절차대로 진행할 수 있다.  
 (1단계) 이용자에게 그들이 만 16세(또는 디지털 동의가 필요한 연령) 이상 또는 미만인지를 진술하도록 요청한다. 해당 이용자가 디지털 동의가 필요한 연령에 해당하는 경우 다음 단계로 진행한다.  
 (2단계) 서비스를 제공하기 위해서는 개인정보 처리에 대한 부모 또는 보호자의 동의나 승인이 필요함을 안내한다. 이 때 이용자에게 부모나 보호자의 이메일 주소를 제공하도록 요청한다.  
 (3단계) 서비스 제공자는 부모나 보호자에게 연락하여 개인정보 처리에 대한 동의를 이메일로 획득한다. 이 때 해당 성인이 부모의 책임을 부담하는 당사자인지 '합리적 수준의 절차'를 거쳐 확인한다.  
 (4단계) 민원이나 이의가 제기될 경우를 대비하여, 서비스 제공자는 아동의 연령을 검증하기 위한 추가 절차를 이행한다.

### 4.3 아동에 대한 통지

GDPR 제12조 및 전문 제58항은 정보주체에게 제공하는 정보를 간결하고 투명하며 쉬운 언어로 작성해야 할 의무는 '특히 아동을 특정하여 제공되는 정보'의 경우 더 엄격히 준수해야 한다고 규정하고 있다.

GDPR 관련 규정

- 제8조(정보사회서비스에 관한 아동의 동의에 적용되는 조건)
- 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식)
- 전문 제38항, 제58항

개인정보보호법 관련 규정

- 제22조(동의를 받는 방법) 제5항

셀프 체크리스트

- |  |                               |                                 |
|--|-------------------------------|---------------------------------|
| • GDPR 적용 대상 국가별 친권자 동의가 필요한 아동 연령기준을 파악하고 있다.         | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
| • 아동 개인정보를 처리하기 위하여 동의를 받아야 할 때에는 부모 등 친권자의 동의를 받고 있다. | <input type="checkbox"/>      | <input type="checkbox"/>        |

## 5

## 민감정보 및 범죄행위 관련 정보 (Special categories of personal data & Personal data relating to criminal convictions and offences)

(제9, 10조)

## Point

- 민감정보의 개념과 범위에 대하여 이해할 수 있다.
- 민감정보의 처리 금지 원칙의 예외 조항에 대하여 이해할 수 있다.

### 5.1 민감정보 처리 금지의 원칙(제9조제1항)

인종·민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체 정보, 건강 정보, 성생활·성적 취향에 관한 정보(이하 '민감정보')의 처리는 금지된다.

### 5.2 민감정보 처리가 가능한 경우(제9조제2항)

컨트롤러와 프로세서는 다음 경우에 한하여 민감정보를 처리할 수 있다.

- ① 정보주체의 명시적 동의(explicit consent)를 획득한 경우(다만 동의에 근거하는 것이 EU 또는 회원국 법률에 의해 금지되지 않은 경우)



- ② 고용, 사회 안보나 사회보장 및 사회보호법(social security and social protection law) 또는 단체협약에 따른 의무의 이행을 위하여 필요한 경우
- ③ 물리적 또는 법적으로 동의를 할 능력이 없는 정보주체의 중대한 이익을 보호하기 위하여 필요한 경우
- ④ 정치·철학·종교 목적을 지닌 비영리 단체나 노동조합이 하는 처리로, 회원이나 전 회원(또는 그 목적과 관련하여 정기적인 접촉을 유지하는 자)에 관해서만 처리하며, 또한 동의없이 제3자에게 공개하지 않는 경우
- ⑤ 정보주체가 일반에게 공개한 것이 명백한 정보
- ⑥ 법적 청구권의 설정, 행사나 방어 또는 법원이 사법적 지위에서 행동하는 데 필요한 경우
- ⑦ 중대한 공익을 위하여 또는 EU나 회원국 법률을 근거로 하는 처리로, 추구하는 목적에 비례하며(proportionate to the aim pursued) 적절한 보호조치가 있는 경우
- ⑧ EU나 회원국 법률 또는 의료 전문가와의 계약을 근거로, 예방 의학이나 직업 의학, 종업원의 업무 능력 판정, 의료 진단, 보건·사회 복지·치료, 보건이나 사회 복지 시스템의 관리 및 서비스 등의 제공을 위하여 필요한 경우
- ⑨ 국경을 넘은 심각한 보건 위협으로부터의 보호 또는 의료 혜택 및 약품이나 높은 수준의 의료장비 확보 등 공중보건 영역에서 공익을 위하여 필요한 경우
- ⑩ 공익을 위한 기록 보존 목적(archiving purposes in the public interest)이나 과학적·역사적 연구 목적, 통계 목적을 위하여 제89조제1항에 따라 필요한 경우

### 5.3 유전정보, 생체 인식 정보 또는 의료 정보

회원국은 GDPR 제9조제4항에 따라 유전정보, 생체 인식 정보 또는 의료 정보에 대하여 추가 조건(한도 포함)을 유지하거나 부과할 권한이 있다.

## 5.4 범죄경력(전과) 및 범죄행위 관련 정보(Criminal convictions and offences)(제10조)

GDPR은 민감정보 유형에 범죄경력 및 범죄행위 정보를 포함하고 있는지에 대하여 구체적으로 명시하고 있지 않다.

그러나 유럽평의회 'Convention 108'<sup>20)</sup>에서 범죄 전과를 민감정보로 본다는 점과, GDPR에서 해당 정보에 대한 처리 규정을 보다 제한적으로 명시한다는 점에서 민감정보로 볼 수도 있다.

그러나 범죄경력 및 범죄행위에 관련한 정보는 민감정보와 달리 원칙적으로 정보주체의 동의에 의해서도 처리가 불가능하기에 이를 구분할 필요가 있다. 제6조제1항에 근거한 범죄경력 및 범죄행위에 관련한 개인정보의 처리 또는 관련 보안조치는 다음의 경우에 한하여만 수행될 수 있다.

- ① 공적 권한의 통제 하에 있을 경우
- ② 적절한 안전장치를 규정하는 EU 또는 회원국의 법이 허가하는 경우

### GDPR 관련 규정

- 제9조(민감정보의 처리)
- 제18조(범죄경력 및 범죄행위 관련 정보)

### 개인정보보호법 관련 규정

- 제23조(민감정보의 처리 제한)

### 셀프 체크리스트

- |                                     |                               |                                 |
|-------------------------------------|-------------------------------|---------------------------------|
| • 민감정보를 임의 수집 및 보유하거나 처리하지 않는다.     | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
| • 민감정보를 처리하는 경우 명확한 법적 근거에 기반하고 있다. | <input type="checkbox"/>      | <input type="checkbox"/>        |

20) EU 집행위원회(1981. 1. 28.), Convention for the Protection of individuals with regard to Automatic Processing of Personal Data.

### 더 알아보기 3

## 투명성의 원칙(Transparency)<sup>21)</sup>

### #1 투명성의 원칙

GDPR은 개인정보를 처리할 때 적법성·공정성과 함께 투명성의 원칙을 준수하도록 명시하고 있습니다. 이 때 투명성의 원칙은 정보주체에게 일련의 정보 처리 과정을 투명하게 알리는 것을 의미합니다.

투명성은 EU 기본권 헌장 제8조에 표명된 개인정보 처리와 관련된 공정성 원칙의 한 가지 표현이며, Directive에서 GDPR에 이르기까지 정보주체의 권리로 강조하고 있는 정보를 제공받을 권리(Right to be informed)와 밀접한 관련이 있다는 점에서 중요합니다.

투명성의 원칙을 준수함으로써 ① 컨트롤러는 정보주체의 개인정보를 적법하고 공정하게 처리하고 있다는 것, ② 컨트롤러가 GDPR과 관련하여 정보주체와 의사소통하고 있다는 것, ③ 컨트롤러가 정보주체의 권리 행사를 지원하고 있다는 것을 제시할 수 있습니다. 이 때 컨트롤러는 정보주체의 개인정보를 투명한 방식으로 처리하고 있다는 사실을 입증할 수 있어야 합니다.

### #2 개인정보의 투명한 처리 입증

제29조 작업반의 투명성 가이드라인은 컨트롤러가 개인정보의 투명한 처리를 입증하기 위하여 다음과 같은 요건을 확인하도록 명시하고 있습니다.

① 간결하고 투명하며, 이해 가능하고 쉽게 접근 가능한 형식

컨트롤러는 정보주체에게 정보를 제공하거나 통지할 때, 프라이버시와 관련되지 않는

21) 제29조 작업반(2018. 1. 23.), Guidelines on transparency under Regulation 2016/679.

다른 정보와 명확하게 구별하여야 합니다. 또한 정보주체가 온라인에서 개인정보보호 정책(privacy statement) 또는 고지(notice)에 대한 특정 이슈를 찾고자 할 때, 전체 내용을 스크롤할 필요 없이 찾고자 하는 특정 섹션으로 이동할 수 있게 하여야 합니다.

컨트롤러는 대상이 되는 정보주체의 평균 이해 수준을 파악하고, 평균 구성원이 이해할 수 있도록 정보를 공개하여야 합니다.

‘쉽게 접근 가능’한 요소는 정보주체가 어렵게 정보를 찾아다닐 필요 없이 해당 정보를 어디에서 접근할 수 있는지 바로 알 수 있어야 한다는 것을 의미합니다. 예를 들면 정보주체에게 직접 정보를 제공하거나, 링크를 제공하거나, 분명한 안내 표시를 하거나, 질문에 대한 답변의 방식을 적용할 수 있습니다.

#### 참고·예시

제29조 작업반은 온라인에서 개인정보를 수집하는 시점에 개인정보보호 정책/고지에 대한 링크를 제공하거나, 또는 개인정보를 수집하는 동일 페이지에서 이를 제공하는 것을 모범사례로 권고한다.

#### ② 명확하고 평이한 언어를 사용

복잡한 문장과 언어 구조를 피하고 되도록이면 간단한 방식으로 정보를 제공해야 한다는 것을 의미합니다.

정보는 구체적이고 확정적이어야 하며, 추상적이거나 모호한 용어(‘may’, ‘might’, ‘some’, ‘often’, ‘possible’ 등의 불확실한 표현)로 표현하거나 달리 해석할 여지를 남겨서는 안 됩니다. 특히 개인정보를 처리하는 목적과 법적 근거가 명확하여야 합니다.

다만 정보주체에게 제공하는 정보에는 지나치게 법률적·기술적·전문적인 언어 또는 용어가 포함되어서는 안 됩니다.

#### ③ 아동에게 정보를 제공할 때

컨트롤러가 아동을 대상으로 상품 또는 서비스를 제공하는 경우, 아동에게 적절하고 공감되는 어휘, 어조, 언어 스타일을 사용하여 아동 자신에게 전달하는 메시지와

정보라는 것을 인지할 수 있도록 보장하여야 합니다.

#### ④ 서면 제공 또는 그 밖의 방식

정보주체에 대한 정보 제공 또는 통지는 기본적으로 문서로 제공하여야 합니다. 다만 GDPR은 전자 수단을 포함하여 명시되지 않은 다른 방식의 사용을 허용합니다.

#### 참고·예시

- 서면 전자 수단과 관련한 제29조 작업반의 입장은 컨트롤러가 웹사이트를 운영하는 경우 웹사이트 방문자 자신이 가장 관심 있는 개인정보보호 정책/고지의 특정 사항으로 이동할 수 있도록 '계층적 개인정보보호 정책/고지(layered privacy statements/notices)'의 사용을 권장하고 있다.
- 그 외 전자적 방식으로 'just-in-time' 상황별 팝업 고지, 3D 터치 또는 호버오버(hover-over)<sup>22)</sup> 고지, 프라이버시 대시보드 등이 포함된다.

#### ⑤ 구두로 정보를 제공할 수 있어야 함

정보주체가 요청한 경우 '구두로(orally)' 정보를 제공할 수 있는데, 이 때 정보주체의 신원 정보는 구두와 다른 수단을 이용하여 증명되어야 한다고 규정하고 있습니다. 제13~14조에 따라 요구되는 구두 정보 제공은 직접 또는 전화와 같이 개인대 개인 방식으로 제공되는 구두 정보를 의미하는 것은 아닙니다. 서면 방식과 더불어 자동화된 구두 정보(automated oral information)를 제공할 수 있는데, 제29조 작업반의 입장은 컨트롤러가 정보주체로 하여금 미리 녹음된 메시지를 다시 들을 수 있도록 해야 한다는 것입니다.

#### ⑥ 무상으로 제공

컨트롤러는 정보주체의 권리 이행과 정보주체에 대한 모든 통지 및 조치에 관하여 정보주체를 대상으로 요금을 청구할 수 없습니다. 이는 정보의 제공이 금융 거래,

22) 호버오버(hover-over) 고지: 마우스의 위치에 정보를 고지할 수 있는 방법을 제공하는 것. 예를 들면 웹사이트에 특정 문장이나 단어 등에 마우스 커서를 위치시키면 고지 내용이 새로운 창으로 보이도록 하는 방법 등으로 구현할 수 있다.

서비스 또는 상품에 대한 지불 또는 구입의 조건이 될 수 없다는 것을 의미합니다. 다만 제12조제5항에 의거하여 정보주체의 요청이 명백한 근거가 없거나 과도한 경우, 특히 그 성격이 반복적인 경우 거부 또는 합리적인 수수료를 부과할 수 있습니다.



## IV. 컨트롤러·프로세서의 역할

1. 컨트롤러(Controller)
2. 대리인(Representatives)
3. 프로세서(Processor)



# 1

## 컨트롤러 (Controller)

### (제24, 26조)

#### Point

- 컨트롤러의 책임과 의무에 대하여 이해할 수 있다.
- 공동 컨트롤러에 대한 개념과 이에 대한 정보주체의 권리를 이해할 수 있다.

#### 1.1 컨트롤러의 책임(Responsibility)(제24조)

컨트롤러는 개인정보 처리의 성격·범위·목적·위험성 등을 고려하여 개인정보의 처리가 GDPR을 준수하여 수행되는 것을 보장하고, 이를 입증할 수 있는 적절한 기술적·관리적 조치(technical and organisational measures)를 이행하여야 한다.

컨트롤러의 의무 준수 입증 요소로서 공인된 행동규약(code of conduct) 또는 인증 제도(certification)가 이용될 수 있다.

#### 1.2 공동 컨트롤러(Joint controller)(제26조)

둘 이상의 컨트롤러가 공동으로 개인정보 처리 목적과 수단을 정하는 경우 공동 컨트롤러가 된다. 이 때 공동 컨트롤러는 당사자 간 합의를 통하여 정보주체의 권리 보장 등 GDPR에 따른 책임에 대하여 각자의 의무를 투명하게 결정하여야 한다.

이러한 컨트롤러 간 합의는 공동 컨트롤러 간 관계를 충분히 반영하여야 하며, 합의의

본질적 내용은 정보주체에게 공개되어야 한다.

정보주체는 합의 내용과 관계 없이 GDPR에 따라 개별 컨트롤러에게 권리를 행사할 수 있다.

#### GDPR 관련 규정

- 제24조(컨트롤러의 책임)
- 제26조(공동 컨트롤러)

#### 셀프 체크리스트

	예	아니오
• 개인정보 처리 시 GDPR 준수를 입증 할 수 있는 적절한 기술적 관리적 조치를 마련하고 이를 이행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 공동 컨트롤러(Joint Controllers)로서 합의한 내용에 대하여 정보주체에게 공개하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 프로세서에 대한 개인정보 교육, 처리 현황 점검 등 관리 활동을 정기적으로 수행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리에 관한 업무를 위탁할 때 개인정보 관리에 관한 책임 사항 등이 포함된 문서(위탁 계약서 등)가 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러는 책임 하에 진행되는 개인정보 처리 활동 및 보유 중인 개인정보 범주에 대하여 기록하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

## 2 대리인 (Representatives) (제27조)

### Point

- 대리인의 서면 지정 의무와 적용 예외 조항을 알 수 있다.
- 대리인의 역할을 이해할 수 있다.

### 2.1 대리인 서면 지정 의무(제27조제1항)

EU 내에 설립되지 않은 컨트롤러 또는 프로세서는 EU 역내 대리인을 서면으로 지정하여야 한다.

### 2.2 적용 예외(제2항)

다음 중 하나의 경우에는 이러한 대리인 지정 의무가 적용되지 않는다.

- 해당 처리가 간헐적으로(occasionally) 발생하고 대규모의 처리가 아니면서, 민감정보 또는 유죄 판결 및 형사 범죄에 관련된 개인정보의 처리를 포함하지 않으며, 개인정보 처리의 성격·상황·범위·목적에 고려하였을 때 개인의 권리와 자유에 대한 위험을 초래할 가능성이 낮은 경우
- 정부부처 또는 관련기관의 경우

## 2.3 대리인의 설립(제3항)

대리인은 정보주체가 거주하고, 재화 또는 서비스를 제공받는 것과 관련하여 개인정보가 처리되거나, 정보주체의 행동이 모니터링되는 회원국 중 한 곳에 설립되어야 한다.

## 2.4 대리인의 권한(제4항)

대리인은 컨트롤러 또는 프로세서와 함께, 또는 이들을 대신하여 GDPR을 준수하기 위한 목적으로 개인정보 처리에 관련된 모든 사안을 진행한다.

### GDPR 관련 규정

- 제27조(EU 내에 설립되지 않은 컨트롤러 또는 프로세서의 대리인)

### 셀프 체크리스트

- |   |                               |                                 |
|---|-------------------------------|---------------------------------|
| • EU 내에 사업장이 없는 경우, EU 내에 위치한 대리인을 서면으로 지정하고 있다.  | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
| • 대리인에게 개인정보처리에 관련된 사항에 대응할 수 있는 책임과 권한을 위임하고 있다. | <input type="checkbox"/>      | <input type="checkbox"/>        |

# 3

## 프로세서 (Processor)

### (제28, 29조)

#### Point

- 프로세서의 지정·대체 조건에 대하여 이해할 수 있다.
- 프로세서가 수행해야 하는 의무에 대하여 알 수 있다.

#### 3.1 (컨트롤러의 서면 승인을 통한) 프로세서의 역할(제28조제1~2항)

프로세서는 컨트롤러의 특정(specific)하거나 일반적인(general) 사전 서면 승인 없이는 다른 프로세서가 업무를 관여하게 할 수 없다. 다만 컨트롤러의 일반 서면 승인의 경우, 프로세서는 다른 프로세서의 추가 또는 대체에 대하여 컨트롤러에게 고지하여 컨트롤러가 이를 반대할 수 있는 기회를 제공하여야 한다.

프로세서는 컨트롤러의 서면 지시에 한하여 개인정보를 처리한다.

컨트롤러는 개인정보를 처리할 때 GDPR을 준수하고, 정보주체의 권리를 보호하는 적절한 기술적·관리적 조치 이행을 보증하는 프로세서만을 이용하여야 한다.

#### 3.2 프로세서의 의무(제28조제3항)

프로세서가 수행하는 개인정보의 처리에는 계약이나 EU 또는 회원국 법률이 적용된다.

이를 통하여 컨트롤러는 프로세서에 대하여 구속력을 갖게 되고, 개인정보 처리의 대상(subject-matter)과 기간·성격·목적·유형 및 정보주체의 유형과 컨트롤러의 권리·의무가 정해진다.

GDPR이 규정하고 있는 프로세서의 의무는 다음과 같다.

- ① 원칙적으로 컨트롤러의 문서화된 지시 사항에 의해서만 개인정보를 처리하여야 한다.
- ② 개인정보를 처리하도록 허가된 자가 비밀유지를 약속하거나 적절한 법정 비밀유지 의무를 적용받도록 보장하여야 한다.
- ③ 개인정보 처리의 보안을 위하여 요구되는 모든 조치를 취하여야 한다.
- ④ 다른 프로세서의 지정과 관련한 규정을 준수하여야 한다.
- ⑤ 컨트롤러가 정보주체의 개인정보 권리를 보장하기 위하여 필요한 조치를 지원하여야 한다.
- ⑥ 회원국 개인정보보호 당국의 승인을 받기 위한 컨트롤러의 활동을 지원하여야 한다.
- ⑦ 컨트롤러와의 관계를 종료할 때 컨트롤러의 선택에 따라 개인정보를 반환 또는 파기하여야 한다. 다만 EU 또는 회원국 법률이 해당 개인정보의 보유를 요구하는 경우에는 예외로 한다.
- ⑧ GDPR 준수 여부를 입증하기 위하여 필요한 모든 정보를 컨트롤러에게 제공하여야 한다. 또한 컨트롤러 또는 컨트롤러가 위임한 다른 감사자가 수행하는 감사를 받아야 하며, 컨트롤러의 지시가 GDPR 또는 다른 회원국의 개인정보보호 규정을 위반한다고 판단되는 즉시 컨트롤러에게 통지하여야 한다.

### 3.3 프로세서 의무 위반(제28조제10항)

프로세서가 처리의 목적 및 수단을 결정함으로써 GDPR을 위반하는 경우, 프로세서는 해당 처리와 관련하여 컨트롤러로 간주되어 그에 상응하는 제재를 받을 수 있다.

### 3.4 프로세서가 컨트롤러를 대신하여 다른 프로세서와 함께 일하는 경우(제28조제4항)

다른 프로세서의 기술적·관리적 조치가 적절한지에 대한 충분한 보증을 제공하여야 한다.

다른 프로세서가 개인정보보호의 의무를 이행하지 않을 경우 프로세서(initial processor)는 다른 프로세서(another processor)의 의무 이행에 대하여 컨트롤러에게 전적인 책임(fully liable)을 진다.

### 3.5 컨트롤러·프로세서의 권한에 따른 처리(제29조)

프로세서와 컨트롤러 또는 프로세서의 권한 하에서 개인정보에 접근할 수 있는 자는 EU 및 회원국 법률에서 요구하지 않는다면 컨트롤러의 지시에 따른 경우를 제외하고 해당 정보를 처리할 수 없다.

#### 참고·예시

##### 컨트롤러와 프로세서 예시<sup>23)</sup>

(예시 1) 이동통신서비스 제공자는 네트워크 트래픽 관리와 과금 기준 설정 등에서 개인정보 처리의 목적과 수단을 규정하는 컨트롤러에 해당한다.

(예시 2) A기업이 신규 판매하는 상품의 이메일 마케팅을 위하여 B, C, D 이메일 마케팅 전문 기업에 A기업의 고객 이메일 주소를 제공하고, 자사 신규 상품의 마케팅 목적으로만 해당 개인정보를 사용하도록 하는 내용의 계약을 체결하는 한편, B, C, D가 마케팅 활동 과정에서 고객 정보를 보호하면서 마케팅 활동을 수행하는지 관리·감독하는 경우

☞ A는 개인정보의 처리 목적과 방식을 결정하는 컨트롤러에 해당하며, B, C, D는 A로부터 지시를 받아 개인정보를 처리하는 프로세서에 해당한다.

(예시 3) 여행사 E가 여행 상품 패키지를 구매한 고객 정보를 항공사 F와 호텔 G에 항공권 및 호텔 예약을 위하여 전달하고, 항공사와 호텔은 요청받은 좌석 및 객실에 대하여 예약을 완료하였으며, 여행사는 고객에게 여행 상품과 관련한 안내 서류와 예약 확인증을 발급한 경우

23) 제29조 작업판(2010. 2. 16.), Opinion 1/2010 on the concepts of “controller” and “processor”, p. 11, 13, 19.

☞ 여행사, 항공사와 호텔은 개인정보 처리에서 각기 다른 고유한 업무 목적을 정하고 이행하며, 그와 관련한 개인정보보호 책임을 부담하는 컨트롤러에 해당한다.

☞ 그런데 이들이 위와 같이 개별적으로 업무를 수행하는 것이 아니라 여행·항공·숙박을 결합한 형태의 인터넷 웹사이트를 공동으로 운영하고 개인정보를 공동으로 활용하며, 보호 책임을 상호 분배하는 방식으로 운영하는 경우에는 공동 컨트롤러(Joint controller)에 해당한다.

※ 다만 동일한 개인정보 처리 활동에 대하여 하나의 주체가 컨트롤러인 동시에 프로세서가 될 수는 없다.<sup>24)</sup>

### GDPR 관련 규정

- 제28조(프로세서)
- 제29조(컨트롤러나 프로세서의 권한에 의한 처리)

### 셀프 체크리스트

	예	아니오
• 개인정보 처리 시 GDPR 준수를 입증 할 수 있는 적절한 기술적 관리적 조치를 마련하고 이를 이행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 취급자에 대한 개인정보 교육, 처리 현황 점검 등 관리 활동을 정기적으로 수행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리에 관한 업무를 위탁할 때 개인정보 관리에 관한 책임 사항 등이 포함된 문서(위탁 계약서 등)가 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 프로세서는 책임 하에 진행되는 개인정보 처리 활동 및 보유 중인 개인정보 범주에 대하여 기록하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

24) ICO, Data Controllers and processors: What difference is and what the governance implications,





## V. 정보주체 권리 강화

---

1. 개요
2. 정보를 제공받을 권리(Right to be informed)
3. 정보주체의 열람권(Right of access by the data subject)
4. 정정권(Right to rectification)
5. 삭제권('잊힐 권리')[Right to erasure('Right to be forgotten')]
6. 처리 제한권(Right to restriction of processing)
7. 개인정보 이동권(Right to data portability)
8. 반대권(Right to object)
9. 프로파일링을 포함한 자동화된 의사결정  
(Automated individual decision-making, including profiling)

# 1

## 개요

GDPR은 제3장(정보주체의 권리)을 통하여 제12~22조 전반에 걸쳐 정보주체의 권리 행사와 강화에 대한 내용을 명시하고 있다.

특히 삭제권('잊힐 권리'), 처리 제한권, 개인정보 이동권 등을 새로 도입하고 열람권, 삭제권('잊힐 권리') 등의 대상을 확대하였다는 점에서 기존 Directive보다 정보주체의 권리 강화 내용을 구체화하였다는 것을 알 수 있다.

[표 5] 정보주체의 권리 강화에 대한 내용 및 관련 주요 조문

No.	정보주체의 권리	관련 조문
1	정보를 제공받을 권리(Right to be informed)	제12-14조
2	정보주체의 열람권(Right of access by the data subject)	제12, 15조
3	정정권(Right of rectification)	제12, 16, 19조
4	삭제권('잊힐 권리')[Right of erasure('Right to be forgotten')]	제13, 17, 19조
5	처리 제한권(Right of restriction of processing)	제12, 18, 19조
6	개인정보 이동권(Right to data portability)	제12, 20조
7	반대권(Right to object)	제12, 21조
8	프로파일링을 포함한 자동화된 의사결정(Automated individual decision-making, including profiling)	제22조

이러한 내용은 컨트롤러가 정보주체의 개인정보를 처리할 때 보다 안전한 기술적·관리적 조치를 취하게 하는 수단으로서 의미가 있으며, 이를 통하여 기업의 책임성을 강화하고 투명성을 입증하는 데 도움이 된다.

## 2

# 정보를 제공받을 권리 (Right to be informed)

### Point

- 정보주체의 요청에 따라 제공해야 하는 정보와 의무적으로 제공해야 하는 정보의 내용 및 제공 시기를 이해할 수 있다.

### 2.1 주요 내용

컨트롤러는 공정하고 투명한 처리 원칙을 보장하기 위하여 정보주체에게 본인의 개인정보 처리에 관한 정보를 어떻게 사용하고 있는지 알려 주어야 한다.

이와 관련하여 GDPR은 컨트롤러가 정보주체에게 제공하여야 하는 정보와 그 시기 및 방법에 대하여 규정하고 있다.

### 2.2 의무적으로 제공하여야 하는 정보(제13~14조)

#### 제공하여야 하는 정보

제공 정보 내용	정보주체에게 직접 수집하는 경우	정보주체에게 직접 수집하지 않는 경우
컨트롤러와 (해당되는 경우) 컨트롤러 대리인과 DPO의 신원 및 연락처	○	○
해당 개인정보의 처리 목적 및 처리의 법적 근거	○	○
(해당되는 경우) 컨트롤러 또는 제3자의 정당한 이익	○	○

개인정보의 유형	-	○
개인정보 수령인 또는 수령인의 유형	○	○
제3국으로 이전한 상세 내용 및 보호 방법	○	○
보유 기간 또는 보유 기간 결정을 위하여 적용한 기준	○	○
정보주체가 갖는 각 권리의 존재	○	○
(해당되는 경우) 언제든지 동의를 철회할 수 있는 권리	○	○
감독기구에 불만을 신청할 수 있는 권리	○	○
개인정보의 출처 및 공개적으로 접근이 허용된 출처인지 여부	-	○
개인정보의 제공이 법률 또는 계약상 요건이나 의무인지 여부 및 개인정보를 제공하지 않을 경우 생길 수 있는 영향	○	-
프로파일링 등 자동화된 결정의 존재 및 어떻게 결정되는 지에 대한 정보와 그 중요성 및 영향	○	○

### 제공 시기

정보주체에게 직접 수집하는 경우	정보주체에게 직접 수집하지 않는 경우
정보를 취득한 때	정보 취득 후 합리적인 기간 내에(최대 1개월) 또는 개인정보가 정보주체와 연락 목적으로 이용되는 경우, 늦어도 해당 정보주체에게 최초로 연락한 시점 다른 수령인에게 공개될 것이 예상된다면, 늦어도 최초로 공개되는 시점

## 2.3 정보주체가 요청한 정보(Request of data subject)(제12조제3항)

### 제공하여야 하는 정보

컨트롤러는 제15~22조에 해당하는 정보주체의 권리 행사를 보장 하여야 한다. 제11조 제2항에 언급된 ‘자신이 정보주체를 식별할 위치에 있지 않음’을 입증하는 경우가 아니라면, 위에 해당하는 정보주체의 권리 행사를 위한 요청을 거절해서는 안 된다.

### 제공 시기

컨트롤러는 제15~22조에 해당하는 정보주체의 요청에 대하여 다음 기준을 준수하여야 한다.

- ① 요청을 접수한 후 한 달 이내 가능한 한 신속하게(without undue delay) 제공한다.
- ② 요청의 복잡성과 요청 횟수를 참작하여, 필요한 경우 2개월 연장하여 제공할 수 있다. 다만 요청을 접수한 지 한 달 이내에 지체 사유와 이러한 연장에 대하여 고지하여야 한다.
- ③ 요청에 대하여 조치를 취하지 않으면, 컨트롤러는 늦어도 접수 후 한 달 내에 미조치 사유, 감독기구에 민원을 제기할 권리, 사법적 구제를 청구할 권리를 정보주체에게 고지하여야 한다.

## 2.4 정보 제공 방법

### 제공 수단(제12조제3항)

정보는 서면으로 제공하여야 하며, 적절한 경우에는 전자적 수단을 포함한 다른 수단을 제공할 수 있다. 정보주체가 요청한 정보의 경우 다른 수단을 통하여 정보주체의 신원이 입증되면 해당 정보는 구두로 제공할 수 있다.

정보주체의 요청이 전자적 형태로 이루어진 경우, 별도의 다른 요청이 없는 한 해당 정보는 가능한 한 전자적 형태로 제공하여야 한다.

### 명확하고 쉬운 언어 사용(제12조제1항)

특히 정보주체가 아동인 경우에는 더욱 간결하고 투명하며 이해하기 쉬어야 하고, 쉽게 접근할 수 있는 방식으로 제공하여야 한다.

### 무상 제공(제12조제5항)

정보에 대한 통지 및 조치는 일체 무상으로 제공되어야 한다. 다만 정보주체의 요청이 명백한 근거가 없거나 과도한 경우, 특히 요청이 반복되는 경우 컨트롤러는 행정적 비용을 고려하여 합리적인 요금을 부과하거나, 해당 요청에 대한 응대를 거부할 수 있다. 다만 요청에 대하여 거부할 때 명백하게 근거가 없거나 과도하다는 사실을 입증할

부담은 컨트롤러에게 있다.

2.5 추가 처리(Further processing)

컨트롤러가 당초 개인정보 수집 목적 이외의 목적으로 개인정보를 추가 처리할 경우, 컨트롤러는 해당 처리 이전에 정보주체에게 관련된 추가 정보를 제공하여야 한다.

GDPR 관련 규정

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제13조(정보주체로부터 개인정보를 수집하는 경우 제공되는 정보)
- 제14조(정보주체로부터 개인정보가 수집되지 않은 경우 제공되는 정보)
- 전문 제58~62항

개인정보보호법 관련 규정

- 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)

셀프 체크리스트

	예	아니오
• 열람·수정·삭제 등 정보주체가 권리를 행사할 때 법령에서 요구하는 제공 시기 및 방법 등을 준수하여 정보주체에게 정보를 제공하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 이용 약관 및 개인정보 처리방침을 쉽게 조회할 수 있도록 정보를 제공하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체로부터 개인정보를 수집하는 경우, 회사가 의무적으로 제공하여야 하는 정보를 개인정보 취득 시점에 즉시 제공하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 제3자가 취득한 개인정보를 제공받을 경우, 의무적으로 제공하여야 하는 정보를 해당 정보주체에게 개별 통지하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 법령 등에 의해 개인정보 처리 목적 외 추가 처리가 필요한 경우, 처리 이전에 정보주체에게 처리 목적에 대한 내용 및 의무적으로 제공하여야 하는 정보를 알려주고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

## 3

## 정보주체의 열람권 (Right of access by the data subject)

### Point

- 정보주체의 열람권에 대한 개념과 열람 가능한 정보의 종류를 이해할 수 있다.
- 열람권 요청에 따른 조치 사항과 제공 방법 및 이행 시기를 이해할 수 있다.

### 3.1 주요 내용(제15조제1항)

컨트롤러는 정보주체가 개인정보 처리가 어떻게 이루어지고 있는지를 알고 그 적법성을 확인할 수 있도록 정보주체의 요구가 있을 경우, 자신의 개인정보 및 다음의 모든 정보에 대하여 열람(access)할 수 있도록 조치하여야 한다.

- ① 처리 목적
- ② 관련된 개인정보의 유형
- ③ 개인정보를 제공받았거나 제공받을 수령인 또는 수령인의 범주
- ④ (가능하다면) 개인정보의 예상 보유 기간 또는 (가능하지 않다면) 해당 기간을 결정하기 위하여 이용하는 기준
- ⑤ 컨트롤러에게 본인의 개인정보에 대한 수정, 삭제 또는 처리 제한이나 처리에 대한 반대를 요구할 수 있는 권리의 유무
- ⑥ 감독기구에 민원을 제기할 수 있는 권리
- ⑦ 개인정보가 정보주체로부터 수집되지 않은 경우 개인정보의 출처에 대한 모든 가용한 정보



- ⑧ GDPR 제22조제1항, 제4항에 규정된 프로파일링 등 자동화된 결정의 유무와 관련 로직에 대한 중요한 정보, 이러한 처리가 정보주체에 미치는 유의성과 예상되는 결과

## 3.2 열람 요구 시 조치 사항(제15조제3항)

### 3.2.1 사본 무상 제공

컨트롤러는 정보주체의 열람 요구에 따라 요청 정보의 사본을 무상으로 제공하여야 한다.

다만 정보주체의 요구에 명백한 근거가 없거나 반복적인 요구 등 과도하다면 이를 거부하거나 '합리적인 요금'을 부과할 수 있다.

### 3.2.2 제공 방법

정보주체의 요구가 전자적 형태로 이루어졌다면, 정보주체가 달리 요구하지 않는 한 일반적으로 이용할 수 있는 전자적 형태로 제공하여야 한다.

컨트롤러는 잠재적 요청(potential request)의 응대라는 유일한 목적만으로 개인정보를 보유해서는 안 된다.

컨트롤러는 '합리적인 방법'을 통하여 열람 요구자의 신원을 확인하여야 한다.

GDPR은 되도록이면 정보주체가 본인의 정보에 직접 접근할 수 있는 방법을 시스템 등을 통하여 원거리 접근이 가능하도록 조치할 것을 권고한다.

다만 이러한 접근 방법이 영업 비밀 또는 지적재산권 및 특히 소프트웨어 보호 저작권 등 다른 사람의 권리와 자유에 악영향을 끼쳐서는 안 된다고 규정하고 있다.

### 3.2.3 이행 시기

컨트롤러는 '가능한 한 신속하게(without undue delay)' 그리고 '늦어도 1개월

이내'에 관련 정보를 제공하여야 한다.

요구가 복잡하거나 다수의 요구일 때에는 이행 기간을 2개월 연장할 수 있다. 다만 이 경우에도 해당 요구를 접수한 날로부터 1개월 이내에 해당 정보주체에게 연장이 필요한 이유를 통지하여야 한다.

#### GDPR 관련 규정

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제15조(정보주체의 열람권)
- 전문 제59항, 제63항, 제64항

#### 개인정보보호법 관련 규정

- 제35조(개인정보의 열람)
- 제38조(권리 행사의 방법 및 절차)

#### 셀프 체크리스트

- |   |                               |                                 |
|---|-------------------------------|---------------------------------|
| • 정보주체가 본인과 관련된 개인정보 처리에 대하여 열람권을 요청하는 경우, 처리 목적, 개인정보 유형 등의 내용 및 조치 사항에 대하여 정보를 제공하고 있다. | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
|---|-------------------------------|---------------------------------|

## 4

# 정정권

## (Right to rectification)

### Point

- 정보주체의 정정권에 대한 개념을 이해할 수 있다.
- 정보주체의 정정권 요청에 따른 조치 사항을 이해할 수 있다.

### 4.1 주요 내용(제16조)

정보주체는 개인정보가 부정확하거나 불완전하다면 이에 대한 정정을 요구할 권리가 있다.

### 4.2 정정 요구 시 조치 사항

컨트롤러는 정보주체의 정정 요구가 있으면 가능한 한 신속하게(without undue delay) 다음과 같이 필요한 조치를 하여야 한다.

- ① 정정 요구를 받은 시점으로부터 1개월 이내에 이행하여야 한다. 다만 정정 요구가 복잡한 경우 2개월 추가 연장이 가능하다.
- ② 정정 요구에 따른 조치를 취하지 않은 경우 정보주체에게 그 이유 및 감독기관에 민원을 제기할 권리와 사법적 구제를 청구할 권리가 있음을 알려 주어야 한다.
- ③ 개인정보를 제3자에게 공개·제공하였다면 가능한 한 그 제3자에게 정정에 대하여 알려 주어야 하며, 적절한 경우 그 정보가 공개된 제3자에 관해서도 정보주체에게

알려 주어야 한다.

#### GDPR 관련 규정

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제16조(정정권)
- 제19조(개인정보의 정정이나 삭제 또는 처리 제한에 관한 고지 의무)

#### 개인정보보호법 관련 규정

- 제36조(개인정보의 정정·삭제)

#### 셀프 체크리스트

- 정보주체가 본인과 관련된 개인정보 처리에 대하여 정정권을 요청하는 경우, 법적 근거에 따라 필요한 조치를 취하고 있다.

예  
☐

아니오  
☐

## 5

### 삭제권('잊힐 권리')

## [Right to erasure('Right to be forgotten')]

#### Point

- 정보주체의 개인정보 삭제권(잊힐 권리)을 이해할 수 있다.
- 삭제권의 보장 범위와 삭제 거부 가능한 경우를 알 수 있다.

#### 5.1 주요 내용(제17조제1항)

정보주체는 컨트롤러에게 본인에 관한 정보의 삭제를 요구할 권리를 가진다.

※ 삭제권은 '잊힐 권리'라고도 하는데, GDPR에서 명시하는 삭제권이 절대적인 '잊힐 권리'를 제공하는 것은 아니다(전문 제65~66항).

컨트롤러는 다음 중 하나에 해당할 경우 정보주체의 삭제권을 보장하여야 한다.

- ① 개인정보가 원래의 수집·처리 목적에 더 이상 필요하지 않은 경우
- ② 정보주체가 동의를 철회한 경우(다만 해당 처리에 대한 법적 사유가 없는 경우)
- ③ 정보주체가 처리에 반대하는 경우로, 처리의 지속을 위한 더 중요한 사유가 없는 경우
- ④ 개인정보가 불법적으로 처리된 경우(GDPR 위반 등)
- ⑤ 법적 의무 준수를 위하여 삭제가 필요한 경우
- ⑥ 아동에게 제공할 정보사회서비스와 관련하여 개인정보를 처리한 경우

## 5.2 삭제 거부 가능한 경우(제17조제3항)

다만 컨트롤러는 다음 중 하나에 해당될 경우에는 삭제 요구를 거부할 수 있다.

- ① 표현 및 정보의 자유에 관한 권리 행사를 위한 경우
- ② 공익적 임무 수행 및 직무권한 행사를 위한 법적 의무 이행을 위한 경우
- ③ 공익을 위한 보건 목적을 위한 경우
- ④ 공익을 위한 기록 보존, 과학적·역사적 연구 또는 통계 목적을 위한 것인 경우
- ⑤ 법적 청구권의 행사나 방어를 위한 것인 경우

## 5.3 공개된 정보(제17조제2항)

컨트롤러가 공개한 개인정보가 제17조제1항에 따라 삭제 의무가 있는 경우, 컨트롤러는 가용한 기술과 비용을 고려하여 개인정보를 처리하는 컨트롤러에게 정보주체의 삭제 요청 사실을 알려야 한다. 특히 온라인 서비스 환경에 종사하는 조직 등 개인정보를 일반에 공개하는 조직은 개인정보를 처리하는 다른 조직에게 해당 개인정보의 링크 및 사본 또는 복제본을 삭제하도록 알려주어야 한다.

### GDPR 관련 규정

- 제17조[삭제권('잊힐 권리')]
- 제19조(개인정보의 정정이나 삭제 또는 처리 제한에 관한 고지 의무)
- 전문 제65항, 제66항

### 개인정보보호법 관련 규정

- 제36조(개인정보의 정정·삭제)

### 셀프 체크리스트

- |   |                               |                                 |
|---|-------------------------------|---------------------------------|
| • 정보주체가 본인과 관련된 개인정보에 대하여 삭제를 요청하는 경우,<br>법적 근거에 따라 요청 사항을 조치하고 있다. | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
|---|-------------------------------|---------------------------------|

## 6

# 처리 제한권

## (Right to restriction of processing)

### Point

- 정보주체의 처리 제한권에 대한 개념을 이해할 수 있다.
- 정보주체의 개인정보 처리 제한 요청에 따른 조치 사항 및 처리 제한을 해지할 때의 조치 사항을 알 수 있다.

### 6.1 주요 내용(제18조)

정보주체는 자신에 관한 개인정보의 처리를 차단하거나 제한할 권리를 갖는다.  
개인정보 처리가 제한되면 컨트롤러는 그 정보를 보유만 할 수 있다.

다음 중 하나에 해당될 경우에 컨트롤러는 정보주체의 개인정보 처리 제한 요구를 이행하여야 한다.

- ① 정보주체가 개인정보의 정확성에 이의를 제기한 경우(개인정보의 정확성을 입증할 때까지 처리를 제한하여야 한다.)
- ② 정보의 처리가 불법적으로 이루어지고, 정보주체가 개인정보의 삭제권에 대한 행사는 반대하였으나, 정보의 사용 제한을 요구한 경우
- ③ 더 이상 개인정보가 필요하지 않지만, 정보주체가 법적 청구권의 행사나 방어를 위하여 그 정보를 요구한 경우
- ④ 컨트롤러의 정당한 이유가 정보주체의 정당한 이유에 우선하는지 여부를 확인할 때 까지 정보주체가 제21조제1항에 해당하는 반대권을 행사하는 경우

또한 자동 파일링 시스템에서의 개인정보 처리 제한은 원칙적으로 개인정보가 추가 처리, 변경되지 않도록 하는 기술적 수단 적용이 필요하다.

전문 제67항은 다음의 방법을 개인정보 처리 제한의 예시로 들고 있다.

- ① 선택된 정보를 임시로 다른 처리시스템으로 이전
- ② 선별된 개인정보를 공개적으로 열람하지 못하도록 하거나 공개된 개인정보를 웹사이트에서 임시로 제거

## 6.2 처리가 가능한 경우

개인정보의 처리가 제한된 경우에도 불구하고 다음 중 하나에 해당되는 경우에는 처리할 수 있다.

- ① 정보주체의 동의가 있는 경우
- ② 법적 청구권의 입증이나 행사, 방어를 위한 경우
- ③ 제3의 개인이나 법인의 권리 보호를 위한 경우
- ④ EU 또는 회원국의 주요한 공익상 이유가 있는 경우

## 6.3 처리 제한 해제 시

컨트롤러는 개인정보 처리 제한을 해제하기로 결정한 때에는 그 사실을 정보주체에게 알려 주어야 한다.

컨트롤러는 개인정보 처리 제한의 확실한 이행을 위하여 필요한 절차를 수립·검토할 수 있으며, 그 개인정보를 수령인에게 공개 또는 제공하였다면 불가능하거나 과도한 노력을 필요로 하지 않는 한 해당 수령인에게 개인정보 처리 제한에 대한 사항을 알려 주어야 한다.



### GDPR 관련 규정

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제18조(처리에 대한 제한권)
- 제19조(개인정보의 정정이나 삭제 또는 처리 제한에 관한 고지 의무)
- 전문 제65항, 제67항

### 개인정보보호법 관련 규정

- 제37조(개인정보의 처리 금지)
- 제38조(권리 행사의 방법 및 절차)

### 셀프 체크리스트

- 정보주체가 본인과 관련된 개인정보 처리 제한을 요청하는 경우, 법적 근거에 따라 개인정보 처리를 제한하고 있다.

예	아니오
<input type="checkbox"/>	<input type="checkbox"/>

## 7

## 개인정보 이동권 (Right to data portability)

### Point

- 개인정보 이동권의 개념과 적용 가능한 상황을 이해하고 있다.
- 정보주체의 개인정보 이동권 요청에 따른 조치 사항을 이해하고 있다.

### 7.1 주요 내용(제20조제1~2항)

정보주체는 컨트롤러에게 제공한 자신에 관한 개인정보를 체계적으로 구성되고, 일반적으로 사용되며, 기계 판독이 가능한 형식으로 제공받을 권리가 있다. 또한 그 정보를 다른 컨트롤러에게 제공할 것을 요구하거나 또는 직접 이전할 수 있다.

개인정보 이동권은 다음 두 조건에 모두 해당하는 경우 적용된다.

- ① 처리가 정보주체의 동의에 근거하거나 계약의 이행을 위한 경우
- ② 처리가 자동화된 수단에 의해 이루어지는 경우

### 7.2 이동권 요구 시 조치 사항

#### 7.2.1 제공 방법

컨트롤러가 정보주체의 개인정보 이동권을 위하여 개인정보를 제공할 때에는 상호운용성(interoperability)을 보장할 수 있도록 다음 사항을 고려하여야 한다.

- ① 개인정보를 구조적이며 보편적으로 사용되는 기계 판독이 가능한 형태\*로 제공한 다(개방형 형태는 CSV 파일을 포함한다).

※ 정보의 특정 요소를 소프트웨어가 추출할 수 있도록 구조화된 것을 의미한다.

- ② 정보는 무료로 제공한다.

- ③ 정보주체의 요구가 있고 또한 기술적으로 가능하다면 해당 개인정보를 한 컨트롤러에서 다른 컨트롤러로 직접 전송할 수 있다.

※ 다만 다른 조직과 기술적 호환성이 있는 처리 시스템을 채택하거나 유지할 필요는 없다.

## 7.2.2 이행 시기

컨트롤러는 정보주체의 개인정보 이전 요구를 받은 때로부터 1개월 이내에 관련 조치를 이행하여야 한다.

다만 요구가 복잡하거나 여러 건의 요구를 받은 경우에는 2개월 추가 연장할 수 있으며, 이 경우 요구를 받은 때로부터 1개월 내에 정보주체에게 이에 대하여 알리고 연장 사유를 설명하여야 한다.

요구에 대한 조치를 취하지 않을 경우 가능한 한 신속하게(without undue delay) 늦어도 1개월 이내에 개인에게 그 사유를 설명하여야 하며, 감독기구에 불만을 신청할 권리 및 사법적 구제를 청구할 권리가 있음을 함께 알려 주어야 한다.

## 7.2.3 고려 사항

컨트롤러는 이동 가능한 개인정보가 인가받지 않은 또는 불법적인 처리와 예상하지 못한 손실, 파괴 또는 손상으로부터 보호하기 위하여 추가 인증, 암호화 등 개인정보에 적절한 보안이 적용되도록 보장하여야 한다.

개인정보 이동권으로 인해 지적재산권이나 영업 비밀 등 다른 사람의 권리가 침해되는

경우에는 이동권에 대한 의무가 적용되지 않는다.

#### GDPR 관련 규정

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제20조(개인정보 이동권)
- 전문 제68항, 제73항

#### 셀프 체크리스트

- 정보주체가 본인과 관련된 개인정보의 이동을 요청하는 경우, 법적 근거에 따라 이동권(회사와 온라인 서비스 간 등) 요청을 조치하고 있다.

예  
☐

아니오  
☐

## 8 반대권 (Right to object)

### Point

- 정보주체의 반대권의 개념과 반대권이 보장되는 상황에 대하여 이해할 수 있다.
- 정보주체의 반대권 요청에 따른 조치 사항을 이해할 수 있다.

### 8.1 주요 내용(제21조)

GDPR은 다음 세 가지 경우에 대하여 정보주체의 반대권을 보장하고 있다.

- ① 직접 마케팅(프로파일링 포함)
- ② 컨트롤러의 정당한 이익 또는 공익적 임무 수행 및 직무권한 행사에 근거한 개인 정보의 처리
- ③ 과학적·역사적 연구 및 통계 목적의 처리

컨트롤러는 정보주체와 최초 연락하는 시점에 반대권에 대한 내용을 알려 주어야 한다. 이러한 사항은 정보주체에게 명시적으로 강조하여야 하며, 다른 정보와 분리하여 분명하게 제시되어야 한다.

### 8.2 반대권 요구 시 조치 사항

#### 8.2.1 직접 마케팅을 위한 처리 시

정보주체의 반대 요구를 접수한 즉시 직접 마케팅(프로파일링 포함)을 위한 개인정보

처리를 중단하여야 한다. 즉 정보주체가 반대한 후에는 절대로 더 이상 직접 마케팅 목적으로 개인정보를 처리할 수 없다.

컨트롤러는 정보주체가 언제라도 직접 마케팅을 위한 처리에 반대 요구를 할 수 있도록 하여야 하며, 이를 무상으로 처리하여야 한다(전문 제70항).

### 8.2.2 정당한 이익 또는 공적 임무 수행 및 직무권한 행사에 근거한 처리 시

정보주체는 자신의 특수한 상황에 대한 이유로 개인정보 처리가 다음 두 가지 특수한 목적에 근거한 경우에 반대권을 행사할 수 있다.

- ① 제6조제1항(e)에 따른 공익을 위한 업무, 공적 권리를 위하여 필요한 개인정보 처리
- ② 제6조제1항(f)에 따른 정당한 이익에 근거한 처리

컨트롤러는 다음 경우가 아닌 한 개인정보의 처리를 중단하여야 한다. 다음에 관한 입증 책임은 컨트롤러에게 있다(전문 제69항).

- ① 정보주체의 이익이나 권리 및 자유보다 더 중요하고 강력한 정당한 근거를 입증할 수 있는 경우
- ② 그 처리가 법적 청구권의 확정, 행사 또는 방어를 위한 것인 경우

### 8.2.3 과학적·역사적 연구 및 통계 목적의 처리인 경우

정보주체는 자신의 특수한 상황에 대한 이유로 본인과 관련된 과학적·역사적 연구 또는 통계 목적의 처리에 반대할 권리를 갖는다.

다만 해당 처리가 공익을 위한 업무 수행을 위하여 필요한 경우는 예외로 한다.

## 8.3 온라인 서비스의 경우: 자동화된 방식으로 이의 제기가 가능해야 함

컨트롤러는 개인정보의 처리 행위가 반대권을 행사할 수 있는 유형에 속하고 또한

온라인으로 이루어진다면 온라인으로 반대 요청을 처리할 수 있는 방법을 제시하여야 한다.

**GDPR 관련 규정**

- 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)
- 제21조(반대권)
- 전문 제69항, 제70항

**셀프 체크리스트**

- |   | 예                        | 아니오                      |
|---|--------------------------|--------------------------|
| • 정보주체의 반대권 행사 요구에 대한 처리 절차 또는 방법을 수립하여 적용하고 있다.    | <input type="checkbox"/> | <input type="checkbox"/> |
| • 온라인 서비스의 경우 정보주체가 온라인으로 반대권 행사 요구를 할 수 있도록 하고 있다. | <input type="checkbox"/> | <input type="checkbox"/> |

# 9

## 프로파일링을 포함한 자동화된 의사결정 (Automated individual decision- making, including profiling)

### Point

- 프로파일링을 포함한 자동화된 의사결정의 개념을 이해할 수 있다.
- 프로파일링을 포함한 자동화된 의사결정 관련 권리의 요청에 따른 조치 사항을 알 수 있다.

## 9.1 주요 내용

### 9.1.1 프로파일링의 개념

프로파일링은 ‘개인의 사적인 측면의 평가, 특히 다음 사항의 분석이나 예측을 위한 모든 형태의 자동화된 처리’를 의미한다(제4조4항).

- 직장 내 업무 수행(performance at work)
- 경제적 상황(economic situation)
- 건강(health)
- 개인적 취향(personal preferences)
- 신뢰성(reliability)
- 태도(behavior)
- 위치(location) 또는 이동 경로(movements)



### 9.1.2 프로파일링을 포함한 자동화된 의사결정의 대상이 되지 않을 권리 (제22조제1항)

정보주체는 본인에 관하여 ① 법적 효력을 초래하거나 ② 이와 유사한 중대한 효과를 미치는 프로파일링을 포함한 자동화된 처리에 의존된 의사결정의 대상이 되지 않을 권리를 갖는다.

① 법적 효력(legal effect) : 결사의 자유, 투표의 자유 등 정보주체의 법적 권리 또는 법적 상태에 영향을 줄 수 있는 것으로 개인의 법적 상태, 권리, 자유, 시민권 등에 변화를 발생시키는 경우나 은행, 보험, 채용 등의 계약 행위

※ 양육·주택 지원 제도 등 국가 사회 보장 제도의 부여 또는 제한, 국경 입국 거부, 통신 요금 미납에 따른 휴대폰 연결 자동 정지 등

② 법적 효과와 유사한 중대한 효과(similarly significant effect) : 정보주체의 법적 권리에 영향을 미치지 않더라도 동등하거나 유사한 의미의 효과를 발생시키는 경우

※ 학교 입학, 세금 감면, 승진 및 보너스 지급 등

이 때 제22조제1항에서 명시하는 자동화된 의사결정이란 인적 개입 없이 기술적 수단(technological means)에 의해서만 이루어지는 완전 자동화 의사결정(solely automated decision-making)을 의미한다.<sup>25)</sup>

※ 개인이 의사 결정 결과를 검토하거나 최종 의사 결정 전에 다른 요소들을 고려한다면 이는 자동화된 처리에만 근거한(based solely on automated processing) 의사 결정에 해당 되지 않음<sup>26)</sup>

즉 정보주체는 오로지 자동 처리에만 근거한 온라인 신용 신청에 대한 거절이나 인적 개입 없이 이루어지는 전자 채용 관행 등에 적용받지 않을 권리를 갖는다(전문 제71항).

25) 제29조 작업반(2018. 2. 6.), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, p7.

26) 제29조 작업반(2018. 2. 6.), 위의 가이드라인, p8.

## 참고·예시

## 온라인 광고 적용 여부

프로파일링 기반 온라인 광고가 GDPR 제22조에서 명시하는 제재 대상에 해당하는지 여부는 온라인 광고가 가진 효과성을 기준으로 다음의 관점에서 판단하여야 한다.

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

이들테면 “서울에 거주하는 여성”과 같은 특정 지역 및 성별 등의 단순 인구 통계학적 정보의 프로필을 기반으로 하는 패션 아웃렛 광고는 법적 효과를 가지거나 법적 효과와 유사한 중요한 효과를 가진 의사 결정이 아닐 수 있다.

또한 성별이나 연령 등에 따라 서비스에서 보이는 상품 배치를 다르게 하는 것은 규제 대상이 아니지만 검색 서비스를 제공하면서 특정 인종에게 차별적인 콘텐츠나 광고를 우선 배치한다면 이는 규제 대상으로 볼 수 있다.

특히, 타깃이 되는 정보주체의 취약성을 판단할 때 일반적으로는 개인에게 영향이 거의 없더라도 특정 취약 계층이나 특정 소수 집단, 특정 유형의 사람에게는 영향을 미칠 수 있다.

※ 예 : 재정이 취약한 사람에게 온라인 도박 광고가 주기적으로 노출되는 경우 도박 사이트에 가입함으로써 잠재적으로 재정 상태가 더욱 악화될 여지가 있음.

## 9.2 적용 예외(제22조제2항)

제22조제1항에서 명시하는 프로파일링을 포함한 자동화된 의사 결정에 대한 규정은 다음의 경우 적용되지 않는다.

- ① 그 결정이 컨트롤러와 정보주체 간 계약의 체결이나 이행을 위하여 필요한 경우
  - 의사결정 과정에서의 인적 오류(human error), 차별 및 권력 남용 최소화 등을 통하여 일관성 또는 공정성이 향상될 것으로 기대되는 경우
  - 신용정보확인 등을 통하여 고객이 재화나 서비스에 대한 지불 불능 위험이 감소하는 경우
- ② 그 결정이 법에 의하여 인정된 경우
  - 사기나 탈세 방지 목적, 서비스 보안 및 신뢰성의 보장 등

### ③ 그 결정이 명시적 동의에 근거한 경우

- 다만, 동의 과정에서 프로파일링을 통한 예상 결과 및 관련 정보를 충분히 제공받아야 하며 선택의 여지 없이 서비스 이용을 위하여 동의가 강제되거나, 고용 관계 등 권력의 불균형이 있는 경우의 동의는 적정 동의 절차로 보기 어렵다.

#### 참고·예시

##### 아동 대상 자동화된 의사 결정

전문 제기항은 아동을 대상으로 하는 프로파일링을 포함한 자동화된 의사결정의 시행을 원칙적으로 금지한다고 규정하고 있다. 그러나 본문 제22조제2항, 예외 조항에 기반해 아동에 대해서도 자동화된 의사결정이 가능하다(아동 대상 사회 복지 제도의 적용 등을 위한 경우 등). 다만, 아동이 일반 정보주체에 비해 취약하다는 점과 전문 제기항의 내용을 고려하여 컨트롤러는 아동의 프로파일링 및 자동화된 의사결정의 시행에 더욱 주의할 필요가 있다. 특히 기업에서의 마케팅 목적의 아동에 대한 프로파일링과 이를 기반으로 하는 맞춤형 광고는 제한되어야 한다.<sup>27)</sup>

##### 민감 정보의 처리

민감정보 기반의 프로파일링과 자동화된 의사결정은 조문 제9조제2항(a)(정보주체의 명시적 동의)과 조문 제9조제2항(g)(다른 법률에서 규정한 경우)에 한하여 허용하도록 규정하고 있다.

## 9.3 자동화된 의사결정 수행 시 조치 사항

GDPR 제22조제2항(a) 및 (c)에 근거하여 자동화된 의사결정을 수행하는 경우 컨트롤러는 정보주체의 권리, 자유, 적법한 이익을 보호하기 위한 적절한 조치를 취하여야 한다.

### 9.3.1 정보주체 권리 보장 사항

컨트롤러가 이를 위하여 정보주체에게 반드시 보장해야 하는 최소한의 권리는 다음과 같다.

27) 제29조 작업반(2018. 2. 6.), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, p26.

- ① 인적 개입을 요구할 권리
- ② 정보주체가 자신의 관점을 표현할 권리
- ③ 그 결정에 대한 설명을 요구할 권리 및 그에 반대할 권리

### 9.3.2 보호조치(Safeguard)

컨트롤러가 프로파일링을 위하여 개인정보를 처리할 때에는 다음과 같은 적절한 보호조치를 적용하여야 한다.

- ① 처리에 적용된 로직에 관한 유의미한 정보 및 그 중요성과 영향을 알려줌으로써 처리의 공정성과 투명성 보장
- ② 프로파일링을 위한 적합한 수학적 또는 통계적 방법 사용
- ③ 오류를 시정하고 실수 위험을 최소화할 수 있는 적절한 기술적·관리적 조치 시행
- ④ 차별적인 결과를 방지하기 위하여 정보주체의 이익과 권리에 대한 위험의 크기에 비례한 개인정보 보호조치 적용(예: 인종 차별 방지 등)

#### 참고·예시

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

컨트롤러가 개인의 대출 신청 평가 및 거절을 위하여 신용 평가 기관(credit reference agency) 및 컨트롤러가 직접 제공된 정보에 기반하여 신용 점수를 계산하는 경우 동 시스템이 공정하고 책임 있는 대출 결정에 도움이 되었음을 설명하고 의사 결정에 도달하기까지 고려된 주요 특징, 정보 출처 등을 설명한다.

※ 대출 신청 양식에 정보주체가 기재한 정보, 연체 기록 등 과거 금융 서비스 이용 기록, 사기 및 연체·파산 등과 같은 공적 기록

또한, 정보주체에 대하여 사용된 신용 평가 점수 산정 방식이 공정하고 효과적이며 편파적이지 않도록 정기적으로 확인하고 있다는 사실 또한 포함하여 안내할 수 있다.

##### 중요성과 영향

보험 회사가 자동화된 의사결정 프로세스를 활용하여 고객의 운전 습관을 모니터링하고 이를 기반으로 보험료를 설정하는 경우 ① 위험한 운전은 높은 보험료를 유발할 수 있다는 사실을 안내하고, ② 급가속 및 급정거 등의 위험한 운전 습관을 가진 운전자와 보통의 운전자를 상호 비교하는 기능을 제공할 수 있다.

9.3.3 개인정보 영향평가(DPIA)<sup>28)</sup>

프로파일링을 포함한 자동화된 의사 결정에 대해서는 컨트롤러의 책임성을 위해 개인정보 영향평가를 실시하여야 한다. 자동화된 의사 결정 없이 프로파일링만 이루어지는 경우라도 심각한 위험의 발생 가능성 등 제35조에서 규정하는 개인정보 영향평가의 요건에 해당되는 경우 영향평가를 실시해야 한다. 프로파일링을 포함한 자동화된 의사 결정에 대해 개인정보 영향평가를 실시하는 경우 다음의 사항을 고려할 수 있다.

- ① 자동화된 의사 결정 프로세스와 관련된 논리 및 존재에 대한 정보 주체 고지
- ② 정보주체 대상 처리의 중요성 및 예상 결과 설명
- ③ 정보주체 대상 자동화된 의사 결정에 반대할 수 있는 수단 제공
- ④ 정보주체 대상 견해를 표명할 권리 허용 등

GDPR 관련 규정

- 제4조(정의)제4항
- 제22조(프로파일링을 비롯한 자동화된 결정)
- 전문 제71조, 제72조

셀프 체크리스트

- |   |                               |                                 |
|---|-------------------------------|---------------------------------|
| • 프로파일링을 포함한 자동화된 의사 결정이 발생하는 경우 정보주체에게 안내하고 있으며, 정보주체의 제한 요청 시 적절한 조치를 취하고 있다. | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
|---|-------------------------------|---------------------------------|

28) 제29조 작업반(2018. 2. 6.), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, p27.

## 더 알아보기 4

## 프로파일링과 자동화된 의사결정 모두에 적용되는 보호 조치

GDPR은 제22조(프로파일링을 포함한 자동화된 의사결정)의 조항을 통해 프로파일링을 포함한 자동화된 의사결정이 정보주체에게 법적 효력 또는 이와 유사한 중대한 효과를 미치는 경우 이를 거부할 수 있도록 명시하고 있습니다.

그러나, 자동화된 의사 결정과 무관하게 프로파일링만 발생하는 경우에도 GDPR 전반에서 규정하는 개인정보 처리에 관한 주요 원칙 및 정보주체 권리 보장을 위한 관련 조항을 준수해야 합니다. 프로파일링만 발생하는 경우나 프로파일링을 포함한 자동화된 의사 결정 모두에 적용되는 조치는 다음과 같습니다.

## #1 정보보호 원칙

원칙	적용 방향
제5조제1항(a) 적법성공정성 투명성의 원칙	- 프로파일링에 대하여 간결, 투명하며 이해하기 용이하고, 접근하기 쉬운 방식으로 정보를 제공해야 함 - 불공평한 프로파일링으로 인하여 정보주체의 거래에 불리함이 없어야 함
제5조제1항(b) 목적 제한의 원칙	- 개인정보 수집 목적 외 다른 목적으로 프로파일링에 활용하는 경우, 별도로 개별적인 동의를 획득하는 등 추가 조치 필요
제5조제1항(c) 개인정보 처리의 최소화	- 프로파일링에 활용되는 개인정보 수집 및 보유 사유를 명확히 입증할 수 있거나, 집합(aggregated) 정보 또는 익명처리(anonymised)된 정보를 사용 하여 적절한 보호조치를 보장해야 함
제5조제1항(d) 정확성의 원칙	- 프로파일링에 사용되는 개인정보가 정확하고 최신의 것인지 지속적으로 검증하는 적절한 방안 도입 필요
제5조제1항(e) 보유 기간 제한의 원칙	- 프로파일링을 위한 개인정보를 지나치게 장기간 유지하는 경우 위험을 초래할 가능성이 있으므로 적정 보유 기간 산정이 필요

## #2 정보주체 권리 보장

원칙	적용 방향
제13조 및 제14조 정보를 제공받을 권리	- 프로파일링의 프로세스가 어떻게 기능하는지 명확하고 간략하게 설명 - 프로파일링을 포함한 자동화된 의사결정 발생 시 ① 프로파일링 사실, ② 프로파일링을 포함한 자동화된 의사 결정 사실에 대한 정보 제공

제15조 열람권	- 프로파일링 및 이에 활용된 정보에 대한 정보주체의 열람권 보장
제16조 정정권	- 프로파일링에 잘못된 개인정보를 활용하는 경우 이에 사용된 정보 및 정보의 부정확성에 대하여 정정 및 이의를 제기할 수 있는 권리 보장 - 추가 개인정보 제공을 통해 프로파일링을 보완할 수 있는 권리 보장
제17조 삭제권	- 정보주체의 동의를 받은 프로파일링에 대하여 정보주체가 동의를 철회할 때, 법적 근거가 있지 않는 한 프로파일링에 사용된 개인정보 및 프로파일링 결과를 모두 삭제해야 함
제18조 처리 제한권	- 프로파일링 및 자동화된 의사 결정 과정의 모든 단계에 개인정보 처리를 차단하거나 제한할 권리를 적용
제21조 반대권	- 프로파일링을 포함한 자동화된 의사 결정 과정에 대해 정보주체가 대상이 되지 않을 수 있는 권리를 보장 - 프로파일링에 대하여 반대권 제기 시 프로파일링 및 자동화된 의사 결정을 중단하고 필요할 경우 관련 정보를 삭제







## VI. 기업의 책임성 강화

---

1. 개요
2. 개인정보 처리 활동의 기록(Records of processing activities)
3. Data protection by design and by default
4. 개인정보 영향평가(Data protection impact assessment)
5. DPO(Data Protection Officer) 지정
6. 행동규약과 인증(Codes of conduct and certification mechanism)

# 1

## 개요

GDPR에서는 기업의 책임성(accountability) 강화를 위한 조항들을 명시하고 있다. 기존의 Directive에서 기업의 책임성 강화는 암묵적인 요구 사항이었으나, GDPR에서는 제5조2항<sup>29)</sup>을 통하여 개인정보 처리에 대한 책임 준수와 그 입증을 구체적으로 요구하고 있다.

특히 개인정보 처리 활동의 기록, Data protection by design and by default, DPO의 지정, 행동규약과 인증에 대한 구체적인 규정은 기존 Directive보다도 구체화된 기업의 책임성을 요구하는 것으로 보인다.

[표 6] 기업의 책임성 강화와 관련한 내용 및 조문

No.	정보주체의 권리	관련 조문
1	개인정보 처리 활동의 기록	제30조
2	Data protection by design and by default	제25조
3	개인정보 영향평가(DPIA)	제35조
4	DPO의 지정	제37~39조
5	행동규약과 인증	제40~43조

기업의 책임성 강화를 위한 위와 같은 조치는 개인정보 침해 및 관련 조항의 위법 위험을 최소화하고 궁극적으로는 정보주체의 개인정보보호 권리를 보장하는 데 의의가 있다.

29) 컨트롤러는 제5조제1항(개인정보 처리에 대한 원칙)의 준수를 책임지고 이를 입증할 수 있어야 한다.

## 2

## 개인정보 처리 활동의 기록 (Records of processing activities)

### Point

- 개인정보 처리 활동 기록이 필요한 경우를 알 수 있다.
- 개인정보 처리 활동을 기록할 때 포함되어야 하는 문서화 내용을 알 수 있다.

## VI

## 기업의 책임성 강화

### 2.1 처리 활동 기록이 필요한 경우(제30조제5항)

#### 2.1.1 기업의 종업원이 250명 이상인 경우

GDPR은 영세 및 중소기업(micro, small and medium-sized enterprise)의 상황을 고려하여, 종업원 수 250명 이상의 기업에 한하여 개인정보 처리 활동을 의무적으로 문서화하고 보유하도록 규정하고 있다.

#### 2.1.2 예외(종업원 수 250명과 무관)

그러나 해당 기업이 수행하는 개인정보의 처리가 다음 중 하나에 해당하는 경우에는 종업원 수와 무관하게 개인정보 처리 활동의 기록이 필요하다.

- ① 정보주체의 권리와 자유에 위협을 초래할 가능성이 있는 개인정보 처리
- ② 민감정보 처리
- ③ 범죄경력 및 범죄행위에 관련된 개인정보 처리

2.2 문서화 내용(제30조제1~2항)

기업은 내부적으로 다음 내용이 포함된 개인정보 처리 활동을 기록·보유하여야 한다.

[표 7] 개인정보 처리 활동의 기록 내용

컨트롤러와 그 대리인의 경우	프로세서와 그 대리인의 경우
① 컨트롤러와 공동 컨트롤러, 컨트롤러의 대리인 및 DPO의 이름과 연락처	① 프로세서(들)와 프로세서가 대행하는 각 컨트롤러 및 컨트롤러·프로세서의 대리인, DPO의 이름과 연락처
② 처리의 목적	② 각 컨트롤러를 대신하여 수행되는 처리의 범주
③ 정보주체의 범주 및 개인정보 범주에 대한 설명	
④ (해당되는 경우) 제3국 또는 국제기구로의 개인 정보 이전의 경우, 이전 방식에 대한 적절한 보호 조치	③ (해당되는 경우) 제3국 또는 국제기구로의 개인 정보 이전의 경우, 이전 방식에 대한 적절한 보호 조치
⑤ (가능한 경우) 보유 기간(the envisaged time limits for erasure of the different categories of data)	
⑥ (가능한 경우) 제32조제1항에 언급된 기술적·관리적 보호조치에 대한 일반적인 설명	④ (가능한 경우) 제32조제1항에 언급된 기술적·관리적 보호조치에 대한 일반적인 설명

GDPR 관련 규정

- 제30조(처리 활동의 기록)
- 전문 제82항

개인정보보호법 관련 규정

- 제29조(안전 조치 의무)

셀프 체크리스트

예

아니오

개인정보 처리 활동(내부 관리 계획)에 대하여 법에서 요구하는 문서화 내용을 포함하여 기록 및 보유하고 있다.

☐

☐

## 3

## Data protection by design and by default

### Point

- Data protection by design and by default의 개념과 장점을 이해할 수 있다.

Data protection by design and by default는 처리 수단의 결정 시점과 처리 당시 시점에서 개인정보보호의 원칙을 적용하는 데 의의가 있다(제25조).

이 때 컨트롤러는 최신 기술, 실행 비용, 개인정보 처리의 성격과 범위, 상황, 목적, 개인정보 처리로 인해 개인의 권리와 자유에 대하여 발생할 수 있는 변경 가능성, 중대성 및 위험성을 고려하여 적절한 기술적·관리적 조치를 취해야 한다.

이러한 조치는 개인정보 처리의 최소화, 정보주체의 권리 보장(통제권 등), 가명처리 등이 해당된다(전문 제78항).

※ 기업이 모든 프로젝트의 초기 단계에서 개인정보보호를 중요한 고려 사항으로 삼고, 전체 라이프 사이클 전반에 걸쳐 개인정보를 보호하도록 권장하고 있다.

또한 컨트롤러는 기본 설정(default)을 통하여 처리 목적에 필요한 범위 내에서 개인정보가 처리될 수 있도록 적절한 기술적·관리적 조치를 이행하여야 한다. 이러한 조치는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보유 기간 및 접근 가능성에 대해서도 적용된다.

Data protection by design and by default의 이행은 정보주체의 개인정보 유출 및 침해에 관련한 위험을 최소화할 수 있고 컨트롤러와 프로세서의 개인정보보호 의무

준수에도 도움이 된다.

GDPR 관련 규정

- 제25조(Data protection by design and by default)
- 전문 제74~78항

셀프 체크리스트

- |  | 예                        | 아니오                      |
|--|--------------------------|--------------------------|
| • 개인정보 처리를 위한 서비스를 설계할 때 보안성 심의를 통하여 개인정보 라이프사이클 전반에 걸쳐 개인정보가 보호될 수 있도록 구현하고 있다. | <input type="checkbox"/> | <input type="checkbox"/> |
| • 개인정보 처리 시스템과 프로세스에 개인정보보호 기본 설정이 반영되어 있는지 점검하고 있다.                             | <input type="checkbox"/> | <input type="checkbox"/> |

## 4

## 개인정보 영향평가 (Data protection impact assessment)

### Point

- 개인정보 영향평가의 개념과 영향평가의 실시 요건을 이해할 수 있다.
- GDPR에서 요구하는 영향평가의 수행 단계를 이해할 수 있다.

## VI

## 기업의 책임성 강화

#### 4.1 일반적으로 개인정보 영향평가 필요한 경우(제35조제1항)

컨트롤러는 특히 새로운 기술을 사용하고 그 처리 유형이 '개인의 권리와 자유에 높은 위험'을 초래할 가능성이 있는 경우, 개인정보를 처리하기 이전에 예상되는 개인정보 처리에 대한 영향평가를 수행하여야 한다.

※ 컨트롤러는 관련 위험 요소의 출처·성격·특성·심각성 등을 고려하여 평가하여야 한다.

따라서 컨트롤러는 '높은 위험'의 처리 활동을 개시하기 전에 그에 관한 영향평가를 실시하였는지 반드시 확인하여야 한다. 영향평가는 조직 내·외부의 다른 사람에 의해 실시될 수 있지만 그 책임은 컨트롤러에게 있다.

개인정보 영향평가에는 특히 위험을 완화하고 개인정보보호를 보장하며, GDPR 준수를 입증하기 위한 보안 조치, 보호조치 및 메커니즘이 포함되어야 한다.

##### 4.1.1 유사한 영향평가 대상에 대한 일괄 처리

유사한 기술에 대하여 다수의 컨트롤러가 영향평가를 받아야 하는 경우 또는 단일



컨트롤러가 동일하지만 다수의 반복되는 기술 적용에 대하여 영향평가를 받아야 하는 경우 한 번의 개인정보 영향평가를 통해 복수의 처리 작업을 일괄적으로 해결할 수 있다.

#### 참고·예시

- 각자 유사한 CCTV 시스템을 설치하는 지방자치단체들의 경우 각자의 별도 컨트롤러에 의한 처리에 대하여 집단적으로 한 번의 영향평가를 실시할 수 있다.
- 철도 운전자(단일 컨트롤러)가 모든 기차역의 비디오 감시에 대하여 한 번의 영향평가를 실시할 수 있다.

## 4.2 개인정보 영향평가를 의무적으로 수행하여야 하는 경우(제35조제3항)

GDPR은 특히 다음 중 하나에 해당하는 경우 개인정보 영향평가를 수행해야 함을 명시하고 있다.

- ① 프로파일링을 포함한 자동화된 처리에 근거한 개인에 대한 체계적이고 광범위한 평가로, 해당 평가를 바탕으로 한 결정이 해당 정보주체에게 법적 효력을 미치거나 이와 유사하게 중대한 영향을 미치는 경우
- ② 민감정보 또는 범죄경력 및 범죄행위 정보에 대한 대규모 처리를 하는 경우
- ③ 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링(예: CCTV)

## 4.3 개인정보 영향평가 포함 내용(제35조제7항)

GDPR은 영향평가에 최소한 다음 내용을 모두 포함하도록 요구하고 있다.

- ① 예상되는 처리(processing)와 목적에 대한 체계적인 기술  
※ (적용되는 경우) 컨트롤러가 추구하는 정당한 이익을 포함한다.
- ② 목적 관련 처리 작업의 필요성과 비례성에 대한 평가
- ③ 정보주체의 권리와 자유에 대한 위협의 평가
- ④ 개인정보의 보호와 GDPR 준수를 입증하기 위한 보안 조치, 보호조치 및 메커니즘 등 위협을 처리할 것으로 예상되는 조치

#### 4.4 개인정보 영향평가의 수행 시기

영향평가는 개인정보 처리 전에 하여야 하며, 개인정보 처리의 기획 단계 중 가장 먼저 시작하여야 한다.

- ① 개인정보 영향평가는 ‘처리 전’에 하여야 하며(제35조제1항 및 제35조제10항, 전문 제90항 및 제93항), 이것은 Data protection by design and by default 원칙과 일치한다(제25조 및 전문 제78항).
- ② 개인정보 처리 활동이 실제로 개시된 후에 업데이트할 필요가 있다는 사실을 이유로 개인정보 영향평가를 지연하거나 실시하지 않는 것은 타당하지 않다. 개인정보 영향평가는 지속적인 과정이며, 변화의 영향을 받는 동적인 처리 작업이다.

#### 4.5 영향평가 결과의 공개

영향평가 결과는 공개되는 것이 바람직하며, 특히 감독기구와 사전협의를 거친 경우 또는 감독기구의 요청에 의한 경우에는 해당 감독기구에 그 결과를 제공하여야 한다.

- ① 개인정보 영향평가 결과의 공개는 GDPR의 법적 요건은 아니며 컨트롤러의 재량 사항이다. 그러나 컨트롤러는 그들의 개인정보 영향평가 결과를 전부 공개할지, 전부 공개가 아니라면 최소한 일부라도 공개할지 검토하여야 한다.
  - 공개의 목적은 신뢰 증대와 책임감 및 투명성을 증명하기 위한 것이므로 사회 구성원들이 영향을 받는 경우에는 개인정보 영향평가 결과를 공개하는 것이 바람직하다.
- ② 개인정보 영향평가 결과를 공개할 때 평가 내용 전체가 포함될 필요는 없다(특히 개인정보 영향평가가 컨트롤러의 보안 위험에 관한 구체적 정보를 제시하거나 또는 영업 비밀이나 상업적으로 민감한 정보를 유출할 수 있을 경우 등). 이 경우 영향평가의 주요 결과 또는 단순 수행 여부를 보고하는 것으로 갈음할 수 있다.
- ③ 개인정보 영향평가 결과, 개인정보의 처리가 높은 위험을 초래할 가능성이 있는 경우 컨트롤러는 그 처리에 대하여 감독기구와 사전에 협의하여야 한다(제36조제3항(e)).

## 4.6 DPO와 협의가 필요한 경우

컨트롤러와 프로세서는 다음과 같은 사항에 대하여 DPO의 조언을 구할 수 있다.

- ① 개인정보 영향평가를 수행할지 여부
  - 영향평가 수행 시 따라야 할 방법
  - 정보주체의 권리와 이익에 대한 위험을 완화시키기 위한 보호조치
- ② 영향평가가 정확하게 수행되었는지 여부와 그 결론이 GDPR을 준수하는지 여부

## 4.7 행동규약의 준수

GDPR은 영향평가를 실시할 때 승인된 행동규약의 준수가 고려되어야 한다고 명시한다(제35조제8항). 승인된 행동규약은 영향평가가 적합한 수단으로서 선택 또는 시행되었음을 입증하는 데 도움이 된다.

## 4.8 감독기구와 사전협의를 필요한 경우(제36조)

개인정보 영향평가 결과, 컨트롤러의 위험 완화 조치가 미비하고 개인정보의 처리가 높은 위험을 초래할 가능성이 있다면 감독기구와 사전에 협의하여야 한다.

위험을 완화하고자 하는 컨트롤러의 조치가 미비 또는 부재한 경우

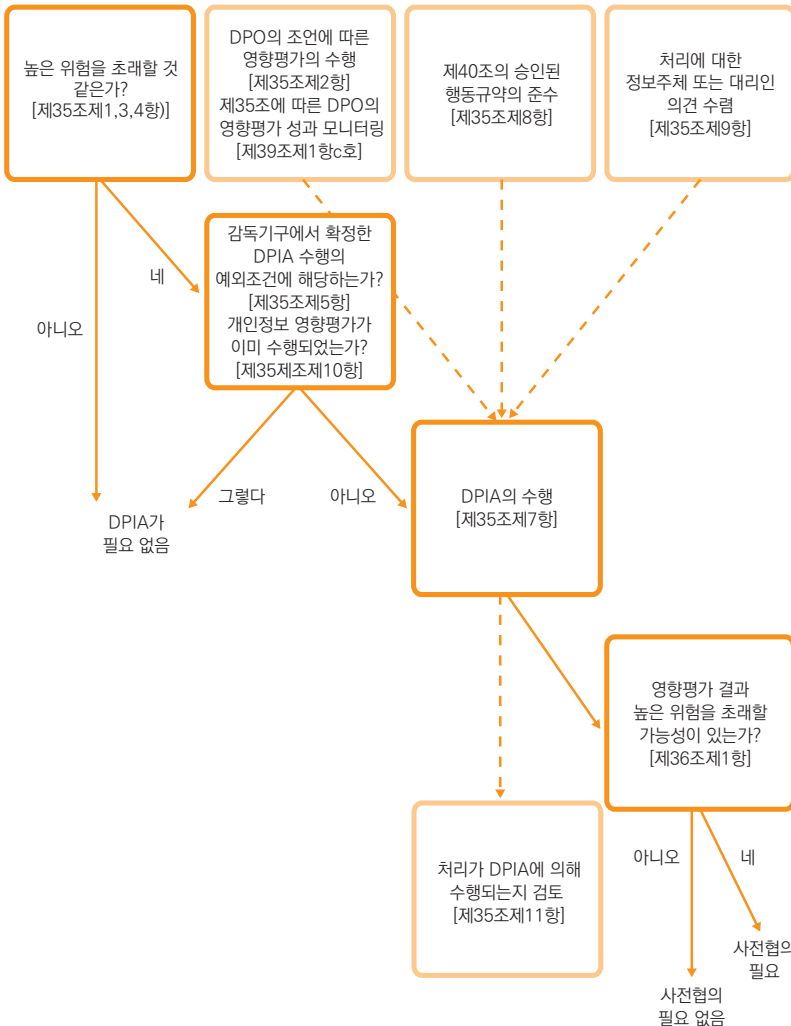
- ① 정보주체의 권리 및 자유에 대한 위험을 평가하는 것, 이러한 위험을 완화하기 위한 수단을 마련하는 것, GDPR의 준수를 증명하는 것은 컨트롤러의 책임이다 [제35조제7항(c)].
- ② 컨트롤러가 위험 완화 조치를 충분히 취할 수 없는 모든 경우에는(위험을 초래할 가능성이 여전히 높을 때에는) 감독기구와의 협의가 필요하다.

해당 개인정보의 처리가 높은 위험을 초래할 수 있는 경우

- ① 높은 위험의 예에는 정보주체가 극복할 수 없는 중대하거나 되돌릴 수 없는 결과에 직면하게 되거나 또는 위험이 발생할 것이 명백한 경우가 포함된다.

- ② 회원국 법률이 공익(사회보장 및 공중보건에 관한 처리를 포함) 과제의 성과 파악을 목적으로 실시된 개인정보 처리에 대하여 컨트롤러에게 감독기구와 협의 또는 사전 승인을 받도록 규정한 경우에는 반드시 감독기구와 협의하여야 한다(제36조제5항).

[그림 2] GDPR의 개인정보 영향평가 수행 단계 흐름도



GDPR 관련 규정

- 제35조(개인정보 영향평가)
- 제36조(사전협의)
- 전문 제89~94항

개인정보보호법 관련 규정

- 제33조(개인정보 영향평가)

셀프 체크리스트

	예	아니오
• 개인정보 처리 유형이 높은 위험을 초래할 가능성이 있는지 여부를 판단하여 개인정보 영향평가 수행여부를 결정하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러는 DPO가 지정되어 있는 경우, 개인정보 영향평가 수행을 위하여 DPO의 조언을 구하고, DPO는 개인정보 영향평가 수행을 모니터링하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 영향평가에 따라 해당 개인정보 처리가 높은 위험을 초래할 가능성이 있는 경우, 컨트롤러는 개인정보 처리 이전에 감독기구에 조언을 구하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

## 5

# DPO(Data Protection Officer)

## 지정

### Point

- DPO를 의무 지정하여야 하는 경우에 대하여 이해할 수 있다.
- DPO의 지정 조건과 역할, 책임에 대하여 알 수 있다.

### VI

### 기업의 책임성 강화

## 5.1 DPO 지정

### 5.1.1 DPO를 반드시 지정하여야 하는 경우(제37조제1항)

컨트롤러와 프로세서는 자유로이 DPO를 지정할 수 있으나, 다음 중 하나의 경우에는 반드시 DPO를 지정하여야 한다.

- ① 정부부처 또는 관련기관의 경우(사법적 권한을 행사하는 법원은 예외)
- ② 컨트롤러 또는 프로세서의 '핵심 활동'이 다음 중 하나에 해당되는 경우
  - 정보주체에 대한 '대규모'의 '정기적이고 체계적인 모니터링'
  - 민감정보나 범죄경력 및 범죄행위 정보에 대한 '대규모'의 처리

### 참고·예시

#### '핵심 활동'의 예시

- ① 병원의 핵심적인 활동은 의료 서비스를 제공하는 것이며, 병원이 환자의 의료 기록과 같은 건강 개인정보를 처리하지 않고서는 안전하고 효율적인 건강 관리를 제공할 수 없다. 그러므로 이러한 개인정보 처리는 병원의 '핵심 활동' 중 하나인 것으로 본다.

- ② 보안 회사의 경우 쇼핑 센터 등 공적인 공간을 감시하며, 불가피하게 개인정보의 처리와 연계되어 있다. 이 때 감시는 보안 회사의 '핵심 활동'으로 본다.

### '대규모 처리'의 예시

- 병원의 정기적인 업무 과정에서 환자 개인정보의 처리
- 교통 시스템을 이용하는 개인들의 이동 개인정보 처리(교통 카드를 통한 추적 등)
- 통계 목적의 패스트푸드 체인 고객의 실시간 지리 위치정보 처리
- 보험 회사 또는 은행의 정기적인 업무 과정에서 고객의 개인정보 처리
- 행동 양식에 따른 맞춤형 광고를 위한 검색엔진의 개인정보 처리
- 전화 또는 인터넷 서비스 제공업체의 개인정보(콘텐츠, 트래픽, 위치) 처리

### '정기적이고 체계적인 모니터링'의 의미 및 예시

- '정기적'은 다음의 하나 또는 그 이상을 의미한다.
  - ① 지속적으로 또는 특정 기간 동안에 특정한 간격으로 발생
  - ② 고정된 주기로 재발하거나 반복
  - ③ 지속적으로 또는 주기적으로 발생
- '체계적'은 다음의 하나 또는 그 이상을 의미한다.
  - ① 시스템에 의하여 발생 및 예정되고, 조직화되거나 또는 규칙적인 경우
  - ② 개인정보 수집을 위한 계획의 일환, 또는 전략의 일부로 수행되는 경우
- 다음의 경우 '정기적'이고 '체계적'인 모니터링 예시에 속한다.
  - ① 모바일 앱을 통한 위치 추적, 고객 보상 프로그램, 행동 양식에 따른 광고의 경우
  - ② 착용형 기기를 통한 건강, 신체 및 의료 개인정보의 모니터링의 경우

다만 GDPR은 DPO 지정 의무와 관련하여 회원국의 개별조항을 통하여 그 범주를 제한할 수 있게 하고 있다.

※ 독일의 경우 개인정보의 자동 처리를 위하여 최소 10명 이상의 인력을 고용하는 컨트롤러는 DPO를 의무 지정하도록 명시하고 있다[Bundesdatenschutzgesetz, BSDG(개정)제38조].

DPO를 지정하거나 또는 지정 요건에 해당하지 않아 지정하지 않는 경우, 그와 같은 결정을 내린 사유를 문서화해야 한다.

DPO 지정 요건에 해당하지 않더라도 DPO를 자발적으로 지정할 수 있다. 다만

자발적으로 DPO를 지정한 경우라도 DPO의 지정·지위·책무 등과 관련한 GDPR 제37~39조가 적용되므로 유의하여야 한다.

### 5.1.2 공동 DPO의 지정(제37조제2항)

GDPR은 ‘각 사업장(establishment)에서 쉽게 접근 가능’할 경우, 사업체 그룹(a group of undertakings)은 1명의 DPO를 지정할 수 있다고 규정하고 있다.

### 5.1.3 외부 DPO의 지정(제37조제6항)

DPO는 컨트롤러 또는 컨트롤러의 직원이거나(내부 DPO), 서비스 계약에 근거하여 직무를 이행할 수 있다. 따라서 DPO는 외부에 존재하는 외부인이 될 수 있으며, 이 경우 개인 또는 조직과 체결한 계약을 바탕으로 그 기능을 수행할 수 있다.

## 5.2 DPO의 자질(제37조제5항)

DPO는 제39조에 명시된 업무를 수행할 수 있는 능력을 바탕으로 지정되어야 한다. 필요한 전문 지식의 수준은 DPO가 수행하는 처리 작업과 보호 수준에 따라 결정되어야 하며, 이는 다음과 같이 제시할 수 있다.

- ① GDPR에 대한 심도 있는 이해 및 자국과 EU 개인정보보호 법률, 관행에 대한 전문 지식
- ② 개인정보 처리 작업에 대한 이해
- ③ 정보 기술 및 보안에 대한 이해
- ④ 기업 및 조직에 대한 지식
- ⑤ 조직 내에서 개인정보보호 문화를 활성화할 수 있는 능력

### 5.3 DPO의 업무(제39조)

DPO는 다음과 같은 업무를 수행하여야 한다.



- ① 컨트롤러와 프로세서 및 임직원에게 GDPR과 다른 개인정보 보호법규의 준수 의무에 대하여 알리고 자문
- ② 내부 정보보호 활동 관리 등 GDPR 및 다른 개인정보 보호법규 이행 상황 모니터링
- ③ 컨트롤러 또는 프로세서에게 정보 제공, 조언 및 권고 사항 제시
- ④ 개인정보 영향평가에 대한 자문 및 평가 이행 감시

## 5.4 DPO의 지위(제38조)

GDPR은 DPO가 개인정보보호와 관련된 모든 문제에 시기적절하게 관여할 수 있도록 보장하여야 한다고 규정한다.

따라서 기업은 DPO가 개인정보보호에 관련한 의견 수렴과 결정에 참여할 수 있도록 보장하고 업무 수행과 전문 지식 보유에 필요한 자원을 제공받을 수 있도록 지원하여야 한다.

개인정보 처리 작업과 활동의 특성 및 조직의 규모에 따라 다음과 같은 자원이 DPO에 제공되어야 한다.

- ① DPO 업무 이행에 대한 고위급 경영진의 적극적 지원
- ② DPO가 자신의 업무를 완수하는 데 필요한 충분한 시간
- ③ 필요할 경우 재정적 자원, 인프라(장소·시설·장비), 구성원의 적절한 지원
- ④ DPO 지명에 대하여 모든 임직원에게 공식적으로 공지
- ⑤ DPO가 조직 내 서비스에 접근할 수 있도록 하여, 해당 서비스로부터 필수적인 지원·정보 등을 받을 수 있도록 조치
- ⑥ DPO의 지속적인 훈련

## 5.5 고용주(employer)의 의무

고용주는 DPO에 대하여 다음과 같은 의무가 있다.

- ① DPO가 기업 조직의 최고 경영층, 즉 이사회에 보고할 수 있도록 할 것
- ② DPO가 독립적으로 임무를 수행할 수 있도록 하며, 그 임무 수행으로 해고나 불이익을 당하지 않도록 할 것
- ③ DPO가 GDPR의 의무 이행을 하기 위하여 적절한 자원을 제공할 것

## 5.6 DPO의 책임 여부

DPO는 GDPR을 준수하지 않는 데 대하여 개인적인 책임을 지지 않는다.

GDPR은 DPO가 아니라 컨트롤러 또는 프로세서가 GDPR을 준수하여 개인정보를 처리하였다는 것을 보장하고, 이를 입증할 수 있는 적절한 기술적·관리적 조치를 이행하여야 한다고 규정하고 있다.<sup>30)</sup>

### GDPR 관련 규정

- 제37조(DPO의 지정), 제38조(DPO의 지위), 제39조(DPO의 업무)
- 전문 제97항

### 개인정보보호법 관련 규정

- 제31조(개인정보 보호책임자의 지정)

### 셀프 체크리스트

	예	아니오
• 컨트롤러 또는 프로세서는 법령에 명시된 DPO 지정 요건에 해당하는 경우, DPO를 지정하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• DPO를 지정한 경우, 컨트롤러 또는 프로세서는 DPO의 연락처 정보를 공개하고, 필요한 경우 감독기구에 통보하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• DPO를 지정한 경우, 법령에서 명시된 DPO의 지위 및 업무 지원 사항을 보장하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• DPO의 업무를 정의하고 DPO는 이를 수행하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

30) 제29호 작업반(2017. 4. 5.), The Guidelines on Data Protection Officer, p. 4.

## 6

# 행동규약과 인증 (Codes of conduct and certification)

### Point

- 행동규약과 인증제도의 의미를 이해할 수 있다.
- 행동규약에 포함할 수 있는 주요 내용을 이해할 수 있다.
- 인증 체계 및 인증기관의 역할을 이해할 수 있다.

## 6.1 행동규약과 인증제도 권장

의무적인 것은 아니지만, GDPR은 기업의 GDPR 준수 입증을 위하여 승인된 행동규약과 인증제도(approved codes of conduct and certification mechanisms)를 이용하도록 권장하고 있다.

행동규약과 인증제도를 채택하는 경우에는 투명성과 책임성 보장이 향상됨은 물론, 위험을 경감하고 제3자와 계약을 체결할 때에도 행동규약 및 인증제도 확인을 통하여 제3자에 대한 개인정보보호 수준을 파악할 수 있다.

## 6.2 행동규약의 작성(제40조)

정부와 감독기구는 행동규약의 작성을 권장할 수 있고, 협회나 대표 단체가 행동규약을 작성할 수 있다. 이러한 행동규약은 정보주체를 포함한 관련 이해관계자들과 협의를 통하여 작성되어 감독기구의 승인을 받아야 한다.

행동규약에는 다음과 같은 내용을 다룰 수 있다.

- ① 공정하고 투명한 개인정보 처리
- ② 특정 상황에서 컨트롤러가 추구하는 정당한 이익
- ③ 개인정보의 수집
- ④ 개인정보의 가명화
- ⑤ 일반 대중 및 정보주체에게 제공되는 정보
- ⑥ 아동에게 제공되는 정보, 그리고 아동에 대한 보호와 부모의 책임을 지닌 자의 아동 관련 동의 획득 방식
- ⑦ 제24조와 제25조에서 규정된 조치 및 절차와 제32조에서 규정된 개인정보 처리의 보안을 보장하는 조치
- ⑧ 감독기구와 정보주체에 대한 개인정보 침해 통지
- ⑨ 개인정보의 제3국이나 국제기구로의 이전
- ⑩ 분쟁 해결 절차

### 6.3 행동규약 준수에 대한 모니터링(제41조)

행동규약과 관련한 전문성을 보유하고 소관 감독기구가 인정한 기관은 행동규약 준수에 대하여 모니터링을 실시할 수 있다.

GDPR은 인정된 기관이 다음 절차를 수립하도록 명시하고 있다.

- ① 해당 컨트롤러와 프로세서의 행동규약 적용 자격을 평가하고, 그들의 행동규약 준수 여부를 감시하며, 정기적으로 그 운영을 검토하는 절차
- ② 행동규약의 위반, 행동규약의 이행이나 이행 방식에 관한 민원을 처리하는 절차와 구조

## 6.4 인증제도(제42조)

회원국, 감독기구, 유럽 개인정보보호이사회(EDPB) 또는 EU 집행위원회는 투명성과 법령 준수를 향상하기 위한 인증제도 수립을 장려하여야 하며, 인증서는 감독기구나 인정된 인증기관이 발행한다.

기업은 인증제도를 통하여 기술적·관리적 조치를 실시하고 있음을 보여 줄 수 있으며, 개인정보 역외 이전의 적절성과 관련된 보호조치를 실시하고 있음을 입증할 수도 있다. 또한 특정 제품이나 서비스의 정보보호 수준 평가를 신속히 할 수 있다.

인증의 최대 유효 기간은 3년이며, 인증 의무를 더 이상 충족하지 않을 경우 인증은 철회될 수 있다.

## 6.5 인증기관(제43조)

인증기관(certification body)은 제3자 적합성 평가 기관(third-party conformity assessment body)으로서, 제42조에 의거한 인증 메커니즘을 운영한다.

개인정보보호와 관련하여 적절한 수준의 전문 지식을 보유한 인증기관은 필요한 경우 제58조제2항(h)에 따른 권한 행사를 허용하도록 감독기구에 고지한 후 인증을 발행, 갱신한다.

인증기관은 컨트롤러나 프로세서의 인증이나 인증 철회를 초래하는 평가에 대하여 책임을 져야 한다.

인증기관에 대한 인정은 최대 5년간 유지되며, GDPR의 요건을 충족하는 경우 동일한 조건으로 갱신될 수 있다.

### 6.5.1 인증기관에 대한 인정<sup>31)</sup>

‘인증기관에 대한 인정’이란 인증기관이 GDPR 제42~43조에 의거하여 인증을 수행할

---

31) 제29조 작업반(2018. 2. 6.), Draft Guidelines on the accreditation of certification bodies under Regulation, pp.8~9.

자격이 있는지 증명하는 것을 의미한다. 즉 인증기관이 인증 활동을 수행(적합성 평가 활동)할 때 적절한 기관인지 인정받을 수 있어야 한다.

회원국은 제43조제1항에 따라 인증기관이 다음의 하나 또는 둘에 의하여 인정되는 것을 보장해야 한다.

- ① 제55조 또는 제56조에 따라 권한있는 감독기구의 자체 요건에 따라 인정
- ② EU 이사회 규칙 (EC) 765/2008 , EN - ISO/IEC 17065/2012 그리고 관련 감독기구의 추가 요건에 따라 지명된 국가 인정 기관이 인정
- ③ 감독기구 및 국가 인정 기관이 모두 인정(두 기관 모두에 인정을 받아야 하는지에 대한 여부는 회원국이 단독으로 결정한다.)

GDPR은 인정기관에 대한 인정에 관하여 새로운 기준을 제시하지는 않는다. 다만 제29조 작업반은 '인증기관에 대한 인정 가이드라인'을 통하여 인정을 위한 추가 요건을 파악할 수 있는 툴 박스를 제공할 것이라고 밝히고 있다.

#### GDPR 관련 규정

- 제40조(행동규약)
- 제41조(승인된 행동규약의 모니터링)
- 제42조(인증)
- 제43조(인증기관)

#### 개인정보보호법 관련 규정

- 제13조(자율 규제에 촉진 및 지원)
- 제32조의2(개인정보보호 인증)

#### 셀프 체크리스트

- |                                       |                               |                                 |
|---------------------------------------|-------------------------------|---------------------------------|
| • 행동규약을 작성하는 경우 감독기구의 승인을 받아 활용하고 있다. | 예<br><input type="checkbox"/> | 아니오<br><input type="checkbox"/> |
|---------------------------------------|-------------------------------|---------------------------------|

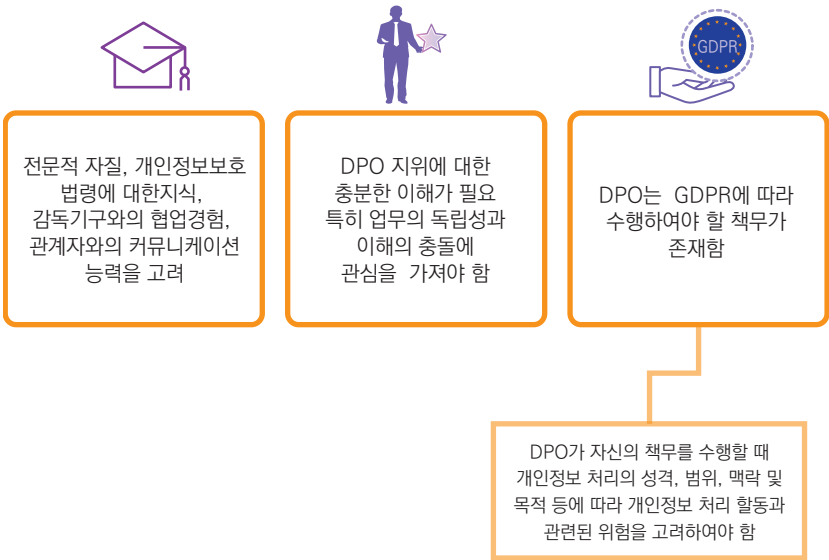
더 알아보기 5

DPO 지정 시 고려 사항<sup>32)</sup> (Designation of a Data Protection Officer)

제29조 작업반은 가이드라인을 통해 DPO의 지정이 GDPR 준수에 중요한 역할을 담당하게 될 것이라고 명시하고 있습니다. GDPR 상에서 특정 컨트롤러와 프로세서는 DPO가 의무 지정 대상이며, DPO의 의무 지정 대상이 아니어도 DPO의 지정은 각 기업의 개인정보보호 관련 의사결정 시 도움이 될 수 있습니다.

따라서 제29조 작업반에서 제시하는 다음의 고려 사항을 참고하여 DPO를 지정하고 업무 프로세스에 적용할 필요가 있습니다.

[그림 3] DPO 지정 시 고려사항



32) 제29조 작업반(2017. 4. 5.), The Guidelines on Data Protection Officer.

## #1 전문적 자질, 개인정보보호 법령에 대한 지식, 감독기구와 협업 경험, 관계자와의 커뮤니케이션 능력

전문적 자질(professional qualities)은 조직이 처리하는 개인정보의 양, 민감도, 복잡도 등에 상응하여야 하지만, 구체적으로 정의내릴 수 있는 개념은 아닙니다. 또한 개인정보 역외 이전의 발생 여부에 따라 보다 높은 전문적 자질이 요구될 수도 있습니다.

DPO가 갖추어야 하는 개인정보보호 법령에 대한 전문 지식(expertise)이 개인정보보호 분야의 자격증 취득이나 박사 학위 등 고학력이나 정보보호 분야에서 일정 기간 이상의 경력을 구체적으로 의미하는 것은 아닙니다. 그러나 이러한 사실들이 전문 지식을 보유한 DPO를 확보하였다는 것을 증명하는 데에 도움이 될 수 있습니다.

DPO는 개인정보보호 감독기구와 협업한 경험을 갖추어야 합니다. 이는 사적으로 감독기구 종사자와 업무 연락을 취할 수 있는 사회적 관계를 요구하는 것이 아닙니다. 개인정보보호 감독기구가 추구하는 정책 목표를 이해하고 감독기구가 작동하는 메커니즘을 이해하여 감독기구와의 협업 과정에서 원활한 의사 소통을 수행할 수 있는 능력이 필요하다는 것을 의미합니다.

DPO는 조직 내부에서만 뿐만 아니라, 감독기구 및 정보주체와도 커뮤니케이션을 수행합니다. 개인정보 처리로 인해 영향받는 다양한 관계자와의 커뮤니케이션을 수행하여야 하기 때문에 그 능력이 필수적으로 요구됩니다. 또한 커뮤니케이션 능력은 EU에서 일반적으로 사용되는 언어 구사 능력이 요구됨을 의미합니다. DPO가 EU의 언어를 직접 구사하지 못하는 경우, 조직은 전문적인 통역 자원을 DPO에게 지원하여야 합니다.

## #2 DPO의 업무 독립성 보장 및 이해 충돌의 방지

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 일으키지 않도록 보장하여야 합니다. 예를 들면 DPO가 정보 처리와 관련한 정책을 설정하는 내부 임직원인 경우 GDPR의 준수보다 비즈니스를 위한 정보 처리의 효율성을 우선적으로 추구할 수 있으며, 이로 인해 이해의 충돌이 발생할 수 있습니다. 컨트롤러나 프로세서는 이와 같은 이해의 충돌이 발생하지 않도록 하여야 합니다.

컨트롤러와 프로세서는 적시에 적절한 방법으로 DPO가 개인정보보호와 관련한 모든 사안에 참여할 수 있다는 것을 보장하여야 합니다. DPO가 GDPR에 규정된 그의 책무를 수행할 때 필요한 자원을 제공하고, 개인정보 처리 활동에 접근할 수 있도록 지원하여야 합니다. 또한 DPO가 전문 지식을 유지할 수 있도록 지원하여야 합니다. DPO가 그의 책무를 효과적이고 효율적으로 이행하는 데 필요한 경우라면 팀을 구성하는 방안도 적극 검토해야 합니다.

### #3 DPO의 책무에 대한 이해

DPO는 다음과 같은 책무를 수행하여야 합니다. 다만 다음 사항은 DPO의 최소 책무에 해당합니다. DPO는 자신의 책무를 수행할 때 개인정보 처리의 성격·범위·맥락·목적 등에 따라 개인정보 처리 활동과 관련된 위험을 고려하여야 합니다(제39조제1항).

- ① 컨트롤러나 프로세서, 개인정보를 처리하는 임직원들에게 GDPR 및 EU 회원국의 개인정보보호 규정에 따른 의무 사항을 알리고 조인
- ② 개인정보의 보호와 관련하여 GDPR 및 EU 회원국의 개인정보보호 규정, 개인정보보호와 관련한 컨트롤러 또는 프로세서의 정책 준수를 모니터링

- ③ 개인정보 영향평가와 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 대하여 감독기구와 접촉 창구 역할 수행
- ⑥ 이 밖에 적절한 경우 다른 사안에 대한 자문 제공

특히 개인정보 영향평가와 관련하여 DPO는 다음 사항에 대하여 조언을 제시하도록 권고됩니다.

- ① 개인정보 영향평가를 수행할지에 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 위하여 적용해야 할 안전 조치
- ⑤ 개인정보 영향평가가 적절히 수행되었는지에 대한 사후 평가

## 더 알아보기 6

### 높은 위험을 초래할 가능성이 있는 개인정보 처리의 판단 기준 9가지

GDPR은 개인정보의 처리가 높은 위험을 초래할 가능성이 있을 경우, 영향평가를 받아 예측되는 위험을 최소화 하도록 권장하고 있습니다.

개인정보 처리 과정에서 높은 위험을 내재하는 개인정보의 판단 기준 9가지는 다음과 같습니다.<sup>33)</sup> 다만, 하나의 기준만을 충족하는 경우 위험 수준이 높다고 보기 힘들며, 적어도 그 이상을 충족하는 개인정보 처리는 영향평가가 필요한 경우로 볼 수 있습니다.

[그림 4] 개인정보 처리 시 높은 위험의 판단 기준



#### #1 평가 또는 평점

정보주체의 업무 성과, 경제적 여건, 건강, 개인적 취향이나 관심, 신뢰도나 자세, 위치나 이동(전문 제71항, 제91항) 등의 데이터를 바탕으로 작성하는 프로필이나 예측을 포함합니다.

33) 제29조 작업반(2017. 10. 4.), Guidelines on Data Protection Impact Assessment(DPIA) and determining whether processing is 'likely to result in a high risk', pp. 8~12.

## #2 법적 효과 또는 이에 유사한 영향을 미치는 자동화된 의사결정

개인에 관련하여 법적(또는 이와 유사한) 영향을 미치는 결정으로 개인정보 처리 알고리즘이 개인에 대한 배격이나 차별로 이어질 수 있는 경우가 이에 해당합니다. 개인에 대한 영향이 적거나 없는 처리는 이 특정 기준에 해당하지 않습니다.

### 참고·예시

온라인 광고가 여성보다 남성에게 보다 높은 임금의 직업 광고를 추천하는 경우 또는 특정 사회의 소수 구성원에게 저렴한 상품을 집중적으로 보여 주는 경우 등

## #3 시스템을 이용한 감시

이 유형의 감시가 기준에 포함되는 이유는 누가 자신의 정보를 수집하는지, 그 정보가 어떻게 이용될지를 정보주체가 모를 수 있는 상황에서 개인정보가 수집되기 때문입니다. 또한 공공장소에서 시스템을 통하여 인지하지 못한 대규모 개인정보 처리의 대상이 되는 것을 피하지 못할 수도 있기 때문입니다.

## #4 민감정보

이것은 제9조에 규정된 민감정보(예를 들면 개인의 정치적 견해에 관한 정보 등)뿐만 아니라 제10조에 규정된 범죄경력이나 범죄행위에 관한 정보도 포함합니다.

### 참고·예시

일반 병원이 환자의 의료 기록을 보유하는 경우, 심부름센터 등이 범죄자의 정보를 보유하는 경우 등

## #5 대규모로 처리하는 정보

GDPR은 무엇이 '대규모 처리'에 해당하는지 명확하게 정의하고 있지는 않습니다.

다만 제29조 작업반은 대규모 처리 여부의 결정에 다음 내용을 고려하도록 권고하고 있습니다.

- ① 관련 정보주체의 수
- ② 처리하는 정보의 양 또는 서로 다른 정보 항목의 범위
- ③ 정보 처리 활동의 기간 또는 영속성
- ④ 처리 활동의 지리적 범위

## #6 연계되거나 결합된 정보

서로 다른 목적을 위하여 또는 서로 다른 컨트롤러에 의해 시행된 둘 이상의 정보 처리 작업을 통하여 얻은 정보를 정보주체의 합리적인 예상을 초과하는 방식으로 연계하거나 결합하는 경우 등이 있습니다.

## #7 취약한 정보주체에 관한 정보

이 유형의 정보 처리는 정보주체와 컨트롤러 간 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 컨트롤러 간 지위 관계의 불균형이 있는 모든 경우도 포함).

### 참고·예시

인적 자원 관리와 연계하여 고용주가 처리하는 종업원의 개인정보 등

## #8 신기술의 사용 또는 적용

물리적 접근 통제 개선 등을 위하여 지문이나 안면 인식을 결합하여 사용하는 것 등이 이러한 사례에 속합니다. GDPR은 새로운 기술이 사용됨에 따라 개인정보 영향평가

실시의 필요를 촉발할 수 있다고 명시합니다(제35조제1항 및 전문 제89항, 제91항). 왜냐 하면 이러한 기술의 이용은 새로운 형태의 정보 수집 및 이용을 내포할 수 있으며, 개인의 권리 및 자유에 대한 높은 위험을 수반할 수 있기 때문입니다.

#### 참고·예시

사물인터넷 관련 기술 적용 등 개인의 일상 생활 및 사생활에 중대한 영향을 줄 수 있는 경우

### #9 처리 자체가 정보주체의 서비스 이용 또는 계약을 방해하는 경우

정보주체의 서비스 접근 또는 계약 체결을 허용·수정·거부하는 것을 목표로 하는 개인정보 처리가 포함됩니다.

#### 참고·예시

은행이 대출 제공 여부를 결정하기 위하여 신용 조회 데이터베이스를 통하여 고객을 심사하는 경우



## VII. 개인정보 역외 이전

---

### 1. 개인정보 역외 이전

(Transfers of personal data to third countries or international organizations)



# 1

## 개인정보 역외 이전 (Transfer of personal data to third countries or international organizations )

### Point

- 개인정보 역외 이전의 개념을 이해할 수 있다.
- EU 밖으로 개인정보 이전이 가능한 규정 조건을 알 수 있다.

### 1.1 개인정보 역외 이전에 관한 총칙

컨트롤러와 프로세서는 제3국이나 국제기구로 개인정보를 이전하거나, 이전 후 처리하는 경우 GDPR에 규정된 요건을 준수하여야 한다.

※ GDPR 내에서 EU 28개 회원국 및 아이슬란드·노르웨이·리히텐슈타인으로 구성되는 EEA(European Economic Area) 간 데이터 이전은 일반적으로 별도의 보호조치가 불필요하다.










여기에는 이전된 개인정보가 다른 제3국이나 국제기구로 재이전되는 경우(onward transfer)도 포함된다. 따라서 역외 이전은 여러 국가에서 비즈니스를 운영하는 기업의 경우 중요한 이슈가 될 수 있다.

개인정보를 역외로 이전하기 위해서는 이전하는 정보의 항목, 정보 제공자(Data exporter), 정보 수령인(Data importer), 이전받는 목적, 정보의 흐름, 적절한 안전 조치 등을 확인하여야 한다.

GDPR상 역외 이전이 가능한 경우는 다음과 같다.

- ① 적정성 결정(Adequacy Decision)
- ② 표준 개인정보보호 조항(Standard Data Protection Clauses)
- ③ 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules)
- ④ 승인된 행동규약(Codes of Conduct) 및 인증제도(Certification mechanism)
- ⑤ 특정 상황에 대한 예외(Derogations for specific situations)

[그림 5] 개인정보 역외 이전 메커니즘

적정성 결정에 따른 이전 (Transfer on the basis of an adequacy decision)	적절한 보호조치에 의한 이전 (Appropriate safeguards)
 <p>집행위원회가 제3국·해당 제3국의 영토나 하나 이상의 지정 부문·국제기구에 대하여 적절한 보호수준을 보장한다고 결정한 경우 제3국 또는 국제기구로의 개인정보 이전이 가능</p> <p>집행위원회는 보호 수준을 평가할 때 EDPB와 협의하고 적정성 결정에 대하여 최소 4년마다 정기적인 검토를 실시하여야 함</p> <p>집행위원회는 적정성 결정을 폐지·개정 또는 정지할 수 있는 권한을 가짐</p>	<p><b>감독기구의 특정한 승인을 요하지 않는 경우</b></p> <ul style="list-style-type: none"> <li> 공공기관 또는 기구 간에 법적 구속력이 있는 강제할 수 있는 장치</li> <li> 제47조에 따른 구속력 있는 기업 규칙</li> <li> 집행위원회가 채택한 표준 개인정보보호 조항</li> <li> 감독기구가 채택하고 집행위원회가 승인한 표준 개인정보보호 조항</li> <li> 제40조에 의거하여 승인된 행동규약</li> <li> 제42조에 의거하여 승인된 인증제도</li> </ul> <p><b>감독기구의 특정한 승인이 필요한 경우</b></p> <ul style="list-style-type: none"> <li> 컨트롤러나 프로세서와 제3국이나 국제기구의 컨트롤러, 프로세서 또는 개인정보 수령인 간의 계약 조항</li> <li> 행정 협정서 내에 강제력 있고 유효한 정보주체 권리 포함 규정</li> </ul>

## 1.2 EU 밖으로 개인정보 이전이 가능한 경우

### 1.2.1 적정성 결정에 따른 이전(Transfer on the basis of an adequacy decision)

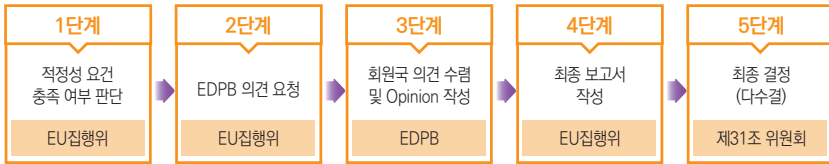
적정성 평가 결과, 집행위원회가 제3국(제3국의 영토, 하나 이상의 지정 부문 포함) 또는 국제기구에 대하여 적절한 보호 수준을 보장한다고 결정한 경우, 제3국 또는

국제기구로의 개인정보 이전이 가능하다.

집행위원회는 보호 수준을 평가할 때 유럽 개인정보보호이사회(EDPB)와 협의하고 적정성 결정에 대하여 최소 4년마다 정기적인 검토를 실시하여야 한다.

또한 집행위원회는 적정성 결정을 폐지·개정·정지 할 수 있는 권한을 갖는다.

[표 8] 적정성 평가 절차



### 1.2.2 적절한 보호조치(Appropriate safeguards)에 의한 이전

컨트롤러나 프로세서가 적절한 보호조치를 제공한 경우에 한하여 정보주체가 행사할 수 있는 권리와 유효한 법적 구제가 제공되는 조건으로 제3국 또는 국제기구에 개인정보를 이전할 수 있다.

#### 1.2.2.1 감독기구의 특정한 승인(Specific authorisation)을 요하지 않는 보호조치

다음과 같은 적절한 보호조치가 적용된 경우에는 감독기구의 특정한 승인이 없이도 역외 이전을 인정받을 수 있다.

- ① 정부부처 또는 관련기관 간 법적 구속력이 있고 강제할 수 있는 장치
  - 정부부처 또는 관련기관 간 법적 효력을 전제로 하는 협약 등을 예시로 들 수 있다.
- ② 제47조에 따른 구속력 있는 기업 규칙(BCRs, Binding Corporate Rules)
  - 다국적 기업이 제47조를 준수한 BCRs를 채택하고 EU 규제 기관에 승인을 받는 경우, 개인정보 이전에 적절한 보호 체계가 갖추어지지 않은 제3국에 위치한 그룹사로 이전하는 것이 가능하다.

## ③ 표준 개인정보보호 조항(Standard Data Protection Clauses)

- 1) 기존의 집행위원회가 채택하거나, 2) 감독기구가 채택하고 집행위원회가 승인한 표준 개인정보보호 조항은 수정·교체·폐지되지 않는 한 그대로 인정된다.
- 다만 표준 개인정보보호 조항을 바탕으로 하는 역외 이전의 경우 감독기구에 통지하거나 승인을 받아야 하는 현행 절차는 폐지되었다.

## ④ 제40조에 따라 승인된 행동규약

- 컨트롤러와 프로세서를 대변하는 기구는 GDPR 적용을 명시할 목적으로 행동규약을 작성·개정·확대할 수 있다.
- 승인된 행동규약이 사용될 경우 적절한 보호조치에 의한 역외 이전으로 인정된다.

## ⑤ 제42조에 따라 승인된 인증제도

- GDPR은 해당 법을 준수하고 있음을 인증하기 위한 목적으로 개인정보보호 인증 메커니즘, 개인정보보호 인장 및 마크의 제정을 장려한다.
- 승인된 인증제도가 사용될 경우 적절한 보호조치에 의한 역외 이전으로 인정된다.

## 1.2.2.2 감독기구의 특정한 승인(Specific authorisation)이 필요한 보호조치

다음과 같은 경우에는 감독기구의 특정한 승인을 받아야 적절한 보호조치로 인정된다.

- ① 컨트롤러나 프로세서와 제3국이나 국제기구의 컨트롤러, 프로세서 또는 개인정보 수령인 사이의 계약 조항
- ② 정부부처 또는 관련기관 간 강제성 있고 유효한 행정 협정서 내 정보주체의 권리를 포함한 규정

1.3 특정 상황에 대한 예외<sup>34)</sup>

적정성 결정, 적절한 보호조치 또는 구속력 있는 기업 규칙이 없는 경우 제3국이나

34) 제29조 작업반(2018. 2. 6.), Guidelines on Article 49, Derogations for specific situation.

국제기구로의 개인정보 이전은 다음 조건에서만 가능하다(제49조제1항).

- ① 정보주체가 적정성 결정 및 적절한 보호조치가 없음으로 인해 정보주체에게 발생할 수 있는 정보 이전에 대한 위험을 고지 받은 후, 정보주체가 이전에 명시적으로 동의한 경우
- ② 정보주체와 컨트롤러 간 계약 이행을 위하여 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위하여 정보 이전을 하여야 하는 경우
- ③ 정보주체의 이익을 위하여 컨트롤러와 그 밖의 개인이나 법인 간 체결된 계약의 이행을 위하여 정보 이전을 하여야 하는 경우
- ④ 중요한 공익상 이유로 정보 이전이 반드시 필요한 경우
- ⑤ 법적 권리의 확립·행사·수호를 위하여 정보 이전이 필요한 경우
- ⑥ 정보주체가 물리적 또는 법률적으로 동의할 수 없는 경우, 정보주체 또는 다른 사람의 중대한 이익을 보호하기 위하여 정보 이전이 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 참조의 조건이 충족되는 범위 내에서 이전되는 경우

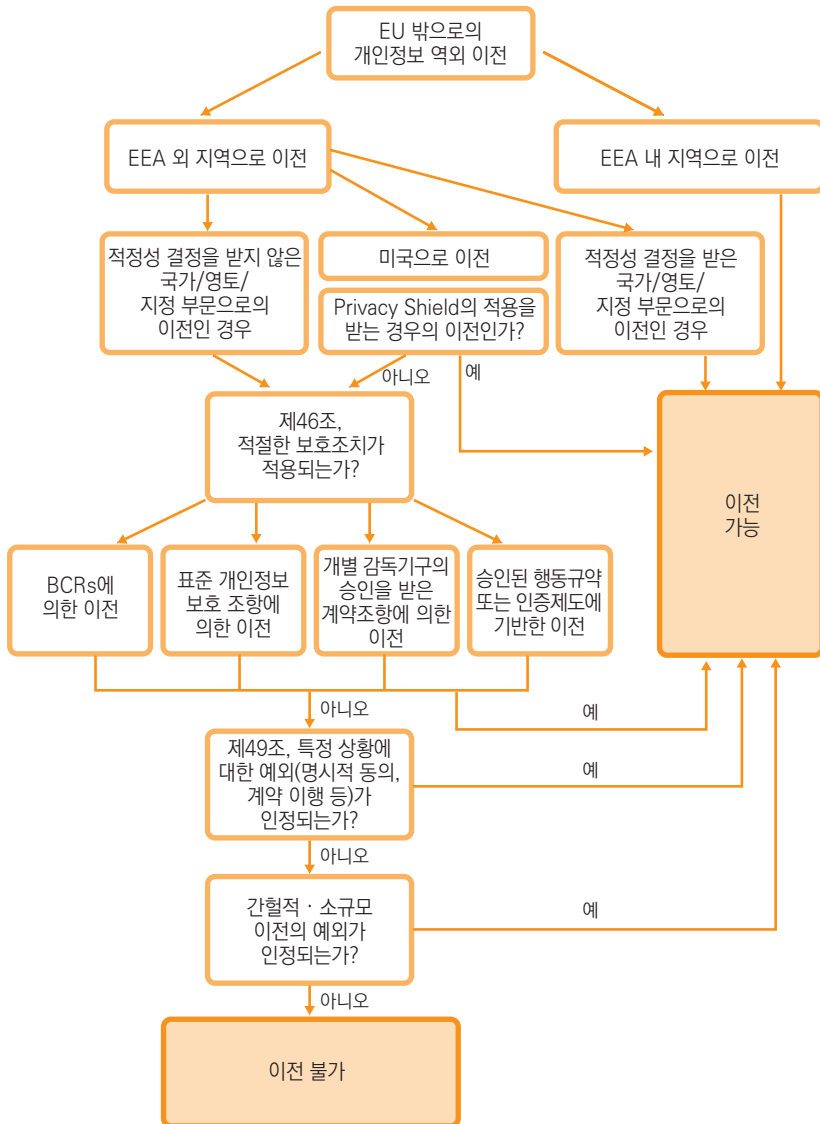
#### 참고·예시

##### 개인정보 역외 이전 시의 명시적 동의<sup>35)</sup>

- 개인정보의 역외 이전에 대한 명시적 동의를 받기 위해서는 정보주체에게 해당 국가 또는 지역으로의 정보 이전이 초래할 수 있는 위험성을 사전에 고지하여야 한다.
- 즉 EU 수준에 부합하는 개인정보보호 체계 및 적절한 보호조치가 부재한 국가로 개인정보가 이전될 것을 알리고, 그로 인해 발생할 수 있는 위험성에 대하여 정보주체가 충분히 인지한 상태에서 유효한 동의의 요건을 충족시켜야 명시적 동의에 의한 개인정보 역외 이전이 이루어질 수 있다.
- 또한 역외 이전 과정에 대한 구체적인 정보\*를 정보주체에게 제공하여야 한다.
  - \* 정보 수령인과 그 유형, 이전되는 정보의 유형, 정보가 이전될 국가 등
- 해당 내용에 대한 명확한 고지와 정보주체의 인지가 전제되어야 정보주체의 명시적 동의에 의한 역외 이전이 가능하다.

35) 제29조 작업반(2018. 2. 6.), Guidelines on Article 49, Derogations for specific situation, pp.6-8.

[그림 6] 개인정보 역외 이전 흐름도<sup>36)</sup>



36) 이 흐름도는 민간부문의 입장에서 개인정보를 역외 이전하는 경우를 대상으로 작성되었다. 다만, 공공부문에서의 개인정보 역외 이전은 추가적인 메커니즘을 고려해야 할 필요가 있다.

위의 조건에 해당되지 않더라도 다음 요건을 모두 만족하는 경우에는 EU 밖으로 이전이 가능하며, 이때 컨트롤러는 개인정보 이전 사실을 감독기구에 고지하여야 한다.

- ① 개인정보 이전이 간헐적이고 한정된 숫자의 정보주체에만 적용되는 경우
- ② 정보주체의 이익이나 권리 및 자유가 우선하지 않는 한, 컨트롤러의 정당한 이익의 목적에 필요한 경우
- ③ 컨트롤러가 개인정보 이전과 관련한 일체의 정황을 평가한 후 그 결과를 토대로 적절한 보호조치를 제시하는 경우

다만 이러한 경우에도 컨트롤러는 의무적으로 해당 감독기구에 이전에 대하여 통지하여야 한다.

#### GDPR 관련 규정

- 제40조(행동규약)
- 제42조(인증)
- 제44조(이전의 일반 원칙)
- 제45조(적정성 결정에 근거한 이전)
- 제46조(적절한 보호조치에 따른 이전)
- 제47조(구속력 있는 기업 규칙)
- 제48조(EU 법이 허가하지 않은 이전 또는 공개)
- 제49조(특정 상황에 대한 예외)
- 전문 제103~114항

#### 개인정보보호법 관련 규정

- 제17조(개인정보의 제공) 제3항

#### 셀프 체크리스트

- |  | 예                        | 아니오                      |
|--|--------------------------|--------------------------|
| • 개인정보를 역외 이전하는 경우, 처리되는 개인정보와 처리 목적을 식별하고 있다.                 | <input type="checkbox"/> | <input type="checkbox"/> |
| • 개인정보를 역외 이전하는 경우, 표준 개인정보보호 조항 등 GDPR에서 허용하는 요건에 의해 이전하고 있다. | <input type="checkbox"/> | <input type="checkbox"/> |

## 더 알아보기 7

**표준 개인정보보호 조항(Standard Data Protection Clauses, SDPC)****#1 표준 개인정보보호 조항**

표준 개인정보보호 조항은 컨트롤러와 컨트롤러 또는 컨트롤러와 프로세서 사이의 개인정보 역외 이전 계약 체결을 위하여 사용되는 통일된 양식의 정보 이전 조항을 의미합니다. 표준 개인정보보호 조항의 양식은 EU 집행위원회에서 채택하였으며, EU의 개인정보보호 원칙을 포함하고 있기 때문에 표준 개인정보보호 조항에 근거한 개인정보 이전은 적정 수준의 보호조치를 보장하고 있는 것으로 인정됩니다.

EU 집행위원회는 총 3가지의 표준 개인정보보호 조항 양식을 채택하고 있습니다.<sup>37)</sup> 두 개는 EU 역내의 컨트롤러-EU 역외의 컨트롤러 간 계약 조항이고, 다른 하나는 EU 역내의 컨트롤러-EU 역외의 프로세서 간 계약 조항입니다.

**#2 표준 개인정보보호 조항의 내용**

표준 개인정보보호 조항의 세부 내용은 EU 개인정보보호 원칙을 명시하고 있으며, 계약서의 유형과 관계 없이 계약 당사자는 공통적으로 다음 내용을 작성하여야 합니다.

- ① 정보 제공자(Data exporter)와 정보 수령인(Data importer)의 연락처 등 기본 정보
- ② 이전되는 정보 유형 및 민감정보·형사 범죄 관련 정보의 포함 여부
- ③ 개인정보 처리의 목적 및 유형 등

또한 표준 개인정보보호 조항의 내용은 계약 당사자 간 필요나 정보 처리 활동의 유형에 따라 변경될 수 있으나, GDPR에 명시된 정보주체의 권리나 처리자의 의무를 준수하여야 합니다.

37) 현재 사용되고 있는 표준 개인정보보호 조항은 EU 집행위원회 홈페이지([http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm))에서 확인할 수 있다. 다만 EC에서는 GDPR의 본격 시행 전, directive에서 명시한 표준계약 조항(Standard Contractual Clauses)이란 용어를 사용하고 있다.



### #3 표준 개인정보보호 조항 기반의 계약 체결 절차

표준 개인정보보호 조항 기반의 계약 체결 절차는 크게 두 단계로 구분되는데, BCRs에 비해 비교적 쉽고 간단합니다.

- ① 회원국의 법규 검토를 통하여 개인정보 수집 및 처리 활동의 적법성 확인(적법한 절차를 통한 개인정보 수집)

※ 이 때 표준계약서에서 전제하고 있는 기술적·관리적 보호조치가 완료되었는지에 대한 검토를 함께 진행하여야 함

- ② 정보 수령인의 유형(컨트롤러 또는 프로세서)을 파악한 후, 해당하는 표준 개인정보보호 조항 기반 계약서 양식을 활용하여 정보 이전 계약 체결

※ 기존 EU Directive에서는 회원국 법률에 따라 계약을 체결한 후에도 별도로 감독기구의 통지나 승인을 요구하는 경우가 있었지만, GDPR은 이러한 절차를 폐지하였음

위의 두 단계를 거쳐 적합한 과정에 따라 표준 개인정보보호 조항 기반의 계약을 체결하면, 해당 계약은 즉시 그 효력을 갖게 됩니다.

### #4 표준 개인정보보호 조항의 장점 및 단점

표준 개인정보보호 조항을 통한 보호조치의 적용은 계약 절차가 간단하며 체결 즉시 계약 내용에 따른 보호조치가 인정된다는 장점이 있습니다. 또한 서로 다른 기업 간 정보 이전을 가능하게 하기 때문에 EU에서 요구하는 역외 이전의 보호조치 중 가장 널리 활용되고 있는 것으로 알려져 있습니다.

그러나 계약 당사자가 많아질 경우 모든 다자간 계약을 체결하여야 하는 부담이 발생할 수 있습니다. 또한 기업 구조 변경 등으로 계약 당사자가 변경되거나, 이전하는 데이터 항목이 확대될 경우 이에 적합한 계약을 다시 체결하여야 합니다.

정보 제공자(Data exporter)와 정보 수령인(Data importer)이 별도의 법인격으로 구분되지 않는 경우에는 계약을 체결하기 곤란하다는 점도 단점으로 꼽힙니다.

※ 예 : 본점과 법인격이 없는 EU 내 지점(branch) 간 개인정보 역외 이전인 경우

## 더 알아보기 8

**구속력 있는 기업 규칙(Binding Corporate Rules, BCRs)****#1 BCRs**

BCRs는 다국적 기업 내부에서 발생하는 개인정보의 역외 이전을 위하여 기업에서 정한 법적 구속력을 갖춘 내부 관리 규정을 의미합니다. 기업에서 채택한 행동규약이 법적 구속력을 갖추기 위해서는 관할 감독기구의 승인이 필요합니다.

기업이 EU의 개인정보보호 원칙을 준수한 행동규약을 작성<sup>38)</sup>하여 감독기구에 승인을 요청하면, 감독기구는 자체 검토 및 유관 감독기구의 회람을 통하여 해당 규칙의 적합성을 판단합니다. 검토 결과 해당 기업 규칙이 개인정보보호에 필요한 조치를 갖추었다고 인정되면, 다른 회원국 감독기구들도 이를 따라 인증하게 되는 시스템입니다.

BCRs는 해당 기업 규칙이 적용되는 기업 집단의 모든 구성원에게 공동으로 적용됩니다. 따라서 다국적 기업이 BCRs를 승인받으면 영업 활동이 진행되고 있는 국가의 보호 수준과 무관하게 개인정보 역외 이전이 가능하게 됩니다.

**#2 유효한 BCRs의 요건**

BCRs가 감독기구로부터 법적 구속력을 인정받기 위해서는 크게 다음 세 가지 기준을 충족시켜야 합니다.

- ① 해당 BCRs가 EU 회원국의 개인정보보호 관련 법률을 준수하고 있음을 사전에 인정
- ② 해당 기업의 모든 사업 부문에 대하여 내부적으로 구속력을 갖고 시행 가능
- ③ 해당 기업의 모든 사업 부문에 대하여 대외적으로 구속력을 갖고 시행 가능

38) BCRs 승인을 위한 표준 양식(Standard application)은 EU 집행위원회 웹사이트에서 받을 수 있다([https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623850](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623850)).

BCRs는 이러한 기준을 바탕으로 작성되어야 하며, 작성 과정에서는 기업의 개인정보보호 관련 업무 담당자와 기술적 구현 가능성을 판단할 수 있는 IT 전문가, 임직원의 대표 및 법무 담당자가 공동으로 참여하는 것이 바람직합니다.

또한 다음과 같은 필수 사항에 대한 명문화가 필요합니다.

- ① 해당 BCRs에 포함되는 기업 집단의 구조와 주요 담당자들의 연락처
- ② 수집하는 개인정보의 범주, 처리의 유형과 목적, 정보주체의 유형 및 이전받는 제3국 담당자의 신원 등 개인정보의 이전 일체에 관한 내용
- ③ 기업 내외부적으로 확보된 법적 구속력과 그 근거
- ④ 피해 구제 및 민원 제기 등 정보주체의 권리와 권리 행사를 위한 수단
- ⑤ 개인정보 열람권을 가진 인력을 대상으로 한 교육 프로그램 등

### #3 BCRs의 승인 절차

기업의 BCRs가 법적 구속력을 갖추기 위해서는 다음 절차에 따라 감독기구의 승인을 받아야 합니다.

- ① BCRs에 대한 법적 인증을 받을 감독기구 선정(해당 감독기구는 주 사업장 및 개인정보 관련 업무를 담당하는 기관의 위치 등을 기준으로 한다.)
- ② 기업의 BCRs 초안 작성 후 감독기구 제출
- ③ 관할 감독기구의 검토 및 유관 감독기구의 회람을 통한 BCRs의 적법성과 필수 요구 사항의 준수 여부 검토
- ④ 감독기구의 BCRs 최종 채택 및 각국 감독기구에 대한 기업의 정보 이전 승인 요청

### #4 BCRs의 장점 및 단점

BCRs는 하나의 기업 집단 내에서 발생하는 개인정보 이전에 대한 포괄적인 적합성을 인정받을 수 있다는 장점이 있습니다. 즉 하나의 기업 집단 전체에 적용되는

보호조치이기 때문에 여러 국가에서 영업 활동을 펼치고 있는 다국적 기업의 정보 이전 활동에 특화되어 있습니다.

그러나 BCRs의 승인을 받는 데 상대적으로 긴 시간이 소요된다는 단점이 있습니다. 또한 그룹 외부의 기업에 대한 적용이 불가하여 별도의 보호조치를 추가로 준비하여야 하는 점도 BCRs의 단점 중의 하나입니다.



## VIII. 개인정보 침해 발생 시 조치 사항

1. 개인정보 침해(Personal data breach)
2. 개인정보 침해 통지(Data breach notification)

# 1

## 개인정보 침해 (Personal data breach)

### Point

- 개인정보 침해의 개념과 위험성을 이해 할 수 있다.

### 1.1 개인정보 침해의 개념

개인정보 침해는 개인정보의 파괴(destruction), 손실(loss), 변경(alteration), 허가받지 않은 공개 또는 접근(unauthorised disclosure or access)<sup>39)</sup>을 일으키는 보안 위반(a breach of security)을 의미한다.

### 1.2 개인정보 침해의 유형

개인정보의 침해는 그 형식에 따라 다음과 같이 구분할 수 있다.

39) ① 파괴: 정보가 더 이상 존재하지 않거나 또는 컨트롤러가 사용할 수 있는 형식으로 존재하지 않는 경우 ② 손실: 데이터가 여전히 존재할 수 있으나 컨트롤러가 그에 대한 제어 또는 접근 권한을 상실하였거나 더 이상 자신의 소유 하에 있지 않은 경우 ③ 변경: 개인정보가 변경되었거나 오염되어 더 이상 완전한 상태가 아닌 경우 ④ 허가받지 않은 공개 또는 접근: 정보 수신(또는 접근) 자격이 없는 수신자에게 개인정보가 공개되는 경우 또는 GDPR을 위반하는 어떠한 형태의 처리

[표 9] 개인정보 침해 유형과 사례

유형	침해 형식	사례
기밀성 침해 (Confidentiality breach)	개인정보에 대한 허가받지 않은 또는 우발적인 공개나 접근이 있는 경우	공격자의 네트워크 침투에 의한 개인정보 접근 또는 유출, 회사 외부에서의 암호화되지 않은 개인정보 사본(CD, USB 등)의 분실·도난 등
가용성 침해 (Availability breach)	개인정보에 대한 허가받지 않은 또는 우발적인 접근 손실이나 파괴가 있는 경우	개인정보의 유일한 사본이 랜섬웨어에 의해 암호화된 경우, 정보가 우발적 또는 비인가자에 의해 삭제되거나 암호화된 정보에 대한 복호화 키가 분실된 경우, 정전 또는 DoS 공격 등으로 조직의 일반적인 서비스에 대한 심각한 중단이 발생하여 항구적 또는 임시적으로 개인정보가 가용하지 않게 되는 경우 등 * 개인정보를 일시적으로 가용하지 못하게 하는 침해의 경우 감독기구 및 개인에 대한 통지 의무는 그 상황에 따라 다를 수 있음
무결성 침해 (Integrity breach)	개인정보에 대한 허가받지 않은 또는 우발적인 변경이 있는 경우	공격자에 의해 개인정보가 변경 또는 오염되었거나, 더 이상 완전한 상태가 아니게 되는 경우 등

### 1.3 개인정보 침해의 위험성

개인정보 침해는 시의적절(timely manner)하게 해결되지 않을 경우, 정보주체의 개인정보에 대한 통제권 상실이나 권리 제한, 차별, 신용 도용 및 신용 사기, 재정적 손실, 가명화의 무단 재식별(unauthorized reversal of pseudonymisation), 명예 훼손, 직무상 비밀, 개인정보의 기밀성 상실과 그 밖에 경제적·사회적 불이익 등과 같은 신체적·물질적·비물질적 피해를 초래할 수 있다(전문 제85항).

이에 GDPR은 컨트롤러 또는 프로세서가 개인정보 침해를 인지하였을 때 감독기구 또는 정보주체에게 통지할 의무를 신설하였다.

### 1.4 개인정보 침해의 인지

개인정보 침해 사고의 ‘인지(aware) 시점’ 기준은 개인정보의 침해로 이어진 보안 사고의 발생을 컨트롤러가 합리적인 수준에서 확신한 때로 본다.



### 참고·예시

#### 개인정보 침해 인지 시점의 예시

- ① 암호화되지 않은 정보가 수록된 CD를 분실하고, 컨트롤러가 CD가 분실된 것을 알게 된 경우
- ② 제3자가 컨트롤러에게 자신이 우연히 컨트롤러의 고객 중 하나의 정보를 입수하였다고 알리고 무단 노출의 명백한 증거를 입수한 경우
- ③ 컨트롤러가 자신의 네트워크에 대한 침입이 있었을 가능성을 발견하고 추가 조사를 통하여 침입 사실을 확인한 경우
- ④ 사이버 범죄자가 대가(ransom)를 요구하기 위하여 시스템을 해킹한 후 컨트롤러에게 접근해 온 경우

### 셀프 체크리스트

- 개인정보 침해 사고의 유형을 인지하고 유형별 사고 대응 절차가 수립되어 있다.

예	아니오
<input type="checkbox"/>	<input type="checkbox"/>

## 2

# 개인정보 침해 통지 (Data breach notification)

### Point

- 개인정보 침해 통지 의무에 대하여 이해할 수 있다.
- 개인정보 침해 사고가 발생하였을 때 통지하여야 하는 대상 및 시기, 내용을 알 수 있다.

## 2.1 감독기구에 대한 통지 의무(제33조)

### 2.1.1 통지 의무

컨트롤러는 개인의 권리와 자유에 위협을 일으킬 가능성이 있는 침해가 발생할 경우 감독기구에 통지하여야 한다.

차별 행위, 평판 훼손, 재정적 손실, 비밀의 누설 또는 다른 심각한 경제적·사회적 불이익 등 개인에게 중대한 악영향을 미칠 수 있는 경우가 이에 해당한다.

### 2.1.2 통지 내용

개인정보 침해 내용을 통지할 때는 최소한 다음 내용을 포함하여야 한다.

- ① 침해 관련 정보주체 및 개인정보 기록의 범주 및 대략적인 개수 등 개인정보 침해 성격
- ② DPO 및 더 많은 정보를 얻을 수 있는 다른 연락처에 대한 이름과 상세 연락처

③ 개인정보 침해로 발생할 수 있는 결과

- ④ 침해로 발생 가능한 부작용을 완화하기 위한 조치 등 해당 개인정보 침해 해결을 위하여 컨트롤러가 취하거나 취하도록 제시된 조치

### 2.1.3 통지 시기

컨트롤러는 개인정보 침해를 인지한 후 가능한 한 신속하게(without undue delay) 72시간 이내에 관련 감독기구에 통지하여야 한다.

72시간을 초과하여 통지가 이루어질 경우 지체된 사유가 함께 통지되어야 하며, 침해 통지와 관련된 정보는 추가 지체(further delay) 없이 단계적(in phase)으로 제공될 수 있다(전문 제85항).

### 2.1.4 통지가 불필요한 경우

컨트롤러가 책임성의 원칙에 따라 해당 개인정보 침해가 개인의 권리와 자유에 위험을 초래할 가능성이 낮다고 입증할 수 있는 경우 감독기구에 대한 통지가 요구되지 않는다(전문 제85항).

※ 개인정보가 이미 공개되어 있고, 이러한 정보의 공개가 개인에 대한 위험을 발생시킬 가능성이 없는 경우 등이 이에 해당한다.

### 2.1.5 프로세서의 통지 의무

프로세서는 개인정보 침해 인지 후 가능한 한 신속하게(without undue delay) 컨트롤러에게 통지하여야 한다.

### 2.1.6 문서화 의무

컨트롤러는 개인정보 침해와 관련된 사실, 그 영향과 취해진 구제 조치 등 모든 개인정보 침해를 문서화하여야 한다.

## 2.2 정보주체에 대한 통지 의무(제34조)

### 2.2.1 통지 의무

컨트롤러는 개인정보의 침해가 개인의 권리와 자유에 대하여 높은 위험을 초래할 가능성이 있는 경우, 정보주체가 필요한 예방 조치(necessary precautions)를 취할 수 있도록 해당 정보주체에게 직접 통지하여야 한다.

### 2.2.2 통지 내용

정보주체에게 통지할 때 개인정보 침해의 성격을 명확하고 평이한 언어로 설명하여야 하며, 최소한 다음 정보가 포함되어야 한다.

- ① DPO 및 더 많은 정보를 얻을 수 있는 다른 연락처에 대한 이름과 상세 연락처
- ② 개인정보 침해로 발생할 수 있는 결과
- ③ 침해로 발생 가능한 부작용을 완화하기 위한 조치 등 해당 개인정보 침해 해결을 위하여 컨트롤러가 취하거나 취하도록 제시된 조치

### 2.2.3 통지 시기

컨트롤러는 침해 행위를 인지한 후 가능한 한 신속하게(without undue delay) 해당 정보주체에게 알려 주어야 한다.

이러한 통지는 감독기구 등이 제공하는 지침을 준수하며, 감독기구와의 긴밀한 협력 아래 합리적으로 가능한 한 신속하게 이루어져야 한다(전문 제86항).

### 2.2.4 통지가 불필요한 경우

다음 중 하나의 경우에는 정보주체에 대한 통지 의무가 면제된다.

- ① 침해 당시 적절한 기술적·관리적 보호조치를 이행하였고, 피해 정보주체에게 해당 조치가 적용된 경우

※ 특히 침해된 개인정보에 접근 권한이 없는 사람이 그 정보를 알 수 없게 만드는 조치인 경우(예: 암호화 정보)

② 컨트롤러가 피해 정보주체의 권리와 자유에 높은 위험을 초래할 가능성이 없도록 만드는 후속 조치를 취한 경우

③ 통지에 과도한 노력이 수반될 수 있는 경우

※ 정보주체가 동등하게 효과적인 방식으로 연락받을 수 있는 공적 연락 수단이나 유사한 조치가 있는 경우 통지 의무를 대신할 수 있다.

2.3 위반 시 과징금

통지 의무를 위반하였을 때 전세계 매출액의 2% 또는 최대 1천만 유로 중 더 큰 금액의 과징금이 부과된다.

GDPR 관련 규정

- 제33조(감독기구에 대한 개인정보 침해 통지)
- 제34조(정보주체에 대한 개인정보 침해 통지)
- 전문 제85~88항

개인정보보호법 관련 규정

- 제34조(개인정보 유출 통지 등)

셀프 체크리스트

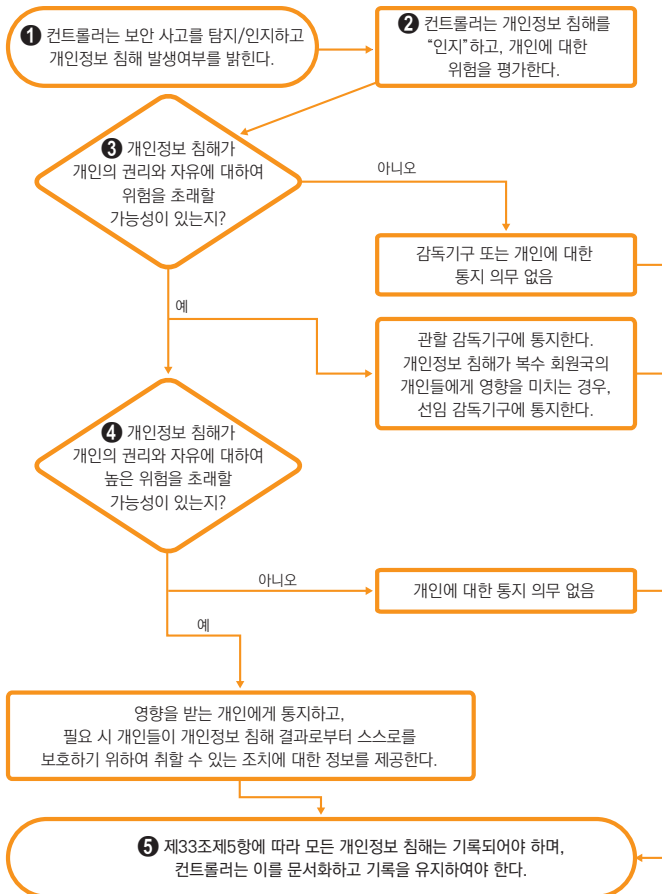
	예	아니오
• 개인정보 침해가 발생하였을 때 가능한 한 신속하게 감독기구에 신고하는 절차가 수립되어 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 침해가 발생하였을 때 프로세서가 인지한 경우 지체 없이 컨트롤러에 통보하는 내용이 위탁 계약서에 포함되어 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 침해가 발생하였을 때 해당 정보주체에게 가능한 한 신속하게 통보할 수 있는 절차를 수립하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러는 개인정보 침해 관련 모든 사항을 문서화하고 있다.	<input type="checkbox"/>	<input type="checkbox"/>

더 알아보기 9

개인정보 침해 통지 흐름도<sup>40)</sup>

제29조 작업반의 데이터 침해 통지 가이드라인은 다음 흐름도를 통하여 개인정보가 침해되었을 때 컨트롤러가 숙지해야 하는 통지 절차를 안내하고 있습니다.

[그림 7] 개인정보 침해 통지 흐름도



40) 제29조 작업반(2018. 2. 6.), Guidelines on Personal data breach notification.

## **#1 보안사고 감지/인지 및 개인정보 침해(personal data breach) 발생 여부 판단 (그림 71의 ①)**

컨트롤러는 개인정보 침해 발생 여부를 즉시 파악하고, 감독기구 및 정보주체에게 통지할 수 있는 모든 적절한 기술적·관리적 대책이 수립되어야 합니다. 개인정보 침해가 발생되었다고 밝혀진 후에 그 위험성에 대한 평가로 이어지게 됩니다.

## **#2 개인정보 침해 인지 및 위험에 대한 평가(그림 71의 ②)**

개인정보 침해가 인지되는 즉시 컨트롤러는 침해 대응 방안과 함께 침해에 대한 위험도를 평가하여야 합니다. 개인에 영향을 미칠 가능성과 심각성을 판단함으로써 효과적인 침해 대응 방안을 수립할 수 있고, 감독기구에 대한 통지 필요 여부를 결정할 수 있습니다.

## **#3 개인의 자유와 권리에 대한 위험을 초래할 가능성에 대한 평가(그림 71의 ③)**

개인정보 침해가 발생하는 경우 컨트롤러는 이를 인지한 때로부터 72시간 내 가능한 한 신속하게 관할 감독기구(선임 감독기구)에게 통지하여야 합니다. 다만, 이는 개인정보 침해가 개인의 권리와 자유에 대하여 위험을 초래할 가능성이 있는 경우에 해당합니다. 컨트롤러는 개인에 대한 심각한 경제적·사회적 불이익 등을 고려하여 위험성 여부를 판단할 수 있으며, 이는 개인정보에 대한 통제력 상실, 권리의 제한, 차별, 신분 도용 또는 사기, 금전적 손실, 익명처리된 정보에 대한 승인되지 않은 식별, 명예 훼손, 직무상 기밀로 보호되는 개인정보의 기밀성 손실 등이 포함됩니다. 평가 결과 위험 초래 가능성이 없는 경우 감독기구 또는 개인에 대한 통지 의무는 없으나, 이후 감독기구에서 위험을 초래할 가능성이 있다고 판단할 경우 컨트롤러는 위험에 대하여 재평가할 필요가 있습니다.

[표 10] 개인정보 침해에 대한 감독기구 통지 필요 여부 판단 예시

통지 필요 여부	예시
통지 불필요	<ul style="list-style-type: none"> <li>- 암호화된 개인정보가 유출되었을 때 암호키의 기밀성이 손상되지 않은 경우 해당 정보는 원칙적으로 파악이 불가능함에 따라 개인에 대한 부정적인 영향을 미칠 가능성이 없으므로 통지 불필요</li> <li>- 비인가자가 해독할 수 없는 방식으로 개인정보가 만들어지고, 정보가 사본이거나 백업이 존재하는 경우, 올바른 방식으로 암호화된 개인정보의 기밀성 침해는 감독기구에 통지 불필요</li> <li>- 언론사 시스템이 정전 등에 의해 몇 시간 동안 차단되어 독자들에게 뉴스를 발송할 수 없는 경우 가용성 침해가 발생한 것이지만 개인의 권리와 자유에 위험을 발생시킨 것으로 볼 수 없으므로 통지 불필요</li> </ul>
통지 필요	<ul style="list-style-type: none"> <li>- 개인정보가 암호화된 경우에도 컨트롤러가 적절한 백업을 하지 않아 손실 또는 변경에 따른 부정적인 영향을 정보주체에게 발생시킬 수 있는 경우 통지 필요</li> <li>- 암호화된 개인정보가 유출되어 통지를 하지 않았으나, 시간이 지남에 따라 키가 훼손된 것으로 확인되거나 암호화 소프트웨어의 취약성이 노출된 경우 통지 필요</li> <li>- 암호화된 정보의 손실이 발생한 침해의 경우 개인정보의 백업이 존재하는 경우에도 백업본으로부터 정보를 복구하는 데 걸리는 시간과 가용성 부족이 개인에게 미치는 악영향이 큰 경우 통지 필요</li> <li>- 병원에서 일시적으로라도 환자의 중요 의료 정보에 접근할 수 없는 경우 수술 취소 등 개인의 권리와 자유에 대한 위험을 발생시킬 수 있으므로 통지 필요</li> <li>- 랜섬웨어 감염에 따라 일시적인 가용성 침해가 발생하더라도 백업본에 의해 신속히 복구가 되었다면 통지가 불필요할 수 있으나, 사고 조사 결과 네트워크 침입을 통하여 기밀성 침해가 함께 발생한 것으로 확인된 경우에는 통지 필요</li> </ul>

#### #4 개인의 권리와 자유에 높은 위험을 초래할 가능성에 대한 평가(그림 7의 ④)

개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우 영향을 받는 개인에게 통지하고 보호조치에 대한 정보를 제공하여야 합니다. 높은 위험에 대한 판단 여부는 개인정보의 성격, 민감도, 개인 식별의 용이성, 개인에게 미치는 영향의 심각도, 개인의 특성, 영향받는 개인의 수, 컨트롤러의 특성 등을 종합적으로 고려하여야 합니다. 컨트롤러는 통지가 지연 없이 이루어졌다는 사실을 입증하여야 하며, 통지가 수행되지 않은 경우 과징금 부과 등 감독기구의 개입이 가능합니다.

[표 11] 개인정보 침해에 대한 정보주체 통지 불필요 예시

통지 필요 여부	예시
통지 불필요	<ul style="list-style-type: none"> <li>- 관리자가 위반 발생 전에 개인정보를 보호하기 위한 적절한 기술적·관리적 조치, 특히 접근 권한이 없는 자가 개인정보를 식별하지 못하도록 하는 대책을 적용한 경우</li> <li>- 위반 발생 즉시 관리자가 개인의 권리와 자유에 대한 심각한 위험이 더 이상 현실화되지 못하도록 조치를 취한 경우</li> <li>- 위반으로 인해 개인의 연락 정보를 분실했거나 알지 못하여 개인과 연락하는 것이 비합리적인 노력의 경우, 이 경우는 위반에 의해 영향을 받을 수 있지만 관리자가 달리 연락할 방법이 없는 경우에 해당한다.</li> </ul>



## #5 제33조제5항에 따른 문서화 및 기록 유지(그림 7의 ㉤)

컨트롤러는 모든 침해 기록과 대응 조치 등에 대한 사항을 문서화하고 기록을 유지하여야 합니다. 이는 감독기구 및 정보주체에 대한 통지 의무와는 관계 없이 내부 관리 대장을 통하여 작성되도록 권고됩니다.





## IX. 피해 구제 및 제재 규정

- 구제 제도(Remedies)
- 손해배상권 및 책임(Right to compensation and liability)
- 과징금(Administrative fines)
- 벌칙(Penalties)

# 1

## 구제 제도 (Remedies)

### (제77~79조)

#### Point

- 개인정보가 침해되었을 때 정보주체가 선택할 수 있는 피해 구제 제도를 이해할 수 있다.

#### 1.1 감독기관에 민원을 제기할 권리(Right to lodge a complaint with a supervisory authority)(제77조)

모든 정보주체는 기존의 행정적·사법적 구제를 받을 권리를 제한 또는 침해받지 않고 감독기관에 민원을 제기할 권리가 있다.

이 경우 정보주체는 거주지나 근무지 또는 침해 발생이 있을 것으로 추정되는 장소가 소재한 회원국의 감독기관에 민원을 제기할 수 있다.

민원을 접수한 감독기관은 민원 처리 경과 및 결과를 민원인에게 알려 주어야 한다.

※ 기존 Directive에 따르면 감독기관은 제기된 민원 관련 개인정보 처리의 적법성을 점검하고, 그 점검 사실을 정보주체에게 통지하는 의무만 부담하였으나, GDPR에서는 민원 처리 경과 및 결과, 그리고 사법적 구제 가능성을 민원인에게 알려 주어야 한다는 점에서 정보주체의 권리가 강화되었다.

#### 1.2 감독기관의 결정에 관한 사법 구제(Judicial remedies against decisions of supervisory authorities)(제78조)

기존의 행정적 또는 비사법적 구제를 제한하거나 침해하지 않고 각 개인 또는 법인은 감독기구의 법적 구속력 있는 결정에 반해 유효한 사법 구제를 청구할 권리가 있다.

또한 감독기구가 민원을 처리하지 않거나, 민원 제기 후 3개월 안에 민원 처리 경과 및 결과를 정보주체에게 알리지 않을 경우 유효한 사법 구제를 구할 수 있다.

전문 제143항은 법원에 이의를 제기할 수 있는 결정 및 조치에는 감독기구의 조사, 시정 및 허가 권한 행사 또는 민원의 기각 또는 각하가 포함된다고 설명하고 있다. 즉 해당 권리는 법적 구속력이 없는 기타 조치(예: 감독기구 발행 의견)를 포함하지 않는다.

### 1.3 컨트롤러 또는 프로세서에 대한 유효한 사법 구제권(Right to an effective judicial remedy against a controller or processor)(제79조)

권리가 침해된 정보주체는 위반 책임이 있는 컨트롤러나 프로세서를 상대로 유효한 사법 구제를 구할 권리가 있다.

기존 Directive에서는 컨트롤러에 대해서만 사법 구제권을 요청할 수 있었던 반면, GDPR에서는 프로세서까지 가능하다는 점에서 정보주체의 권리가 강화되었다고 볼 수 있다.

컨트롤러 또는 프로세서를 상대로 한 법적 절차는 해당 컨트롤러 또는 프로세서의 사업장이 있는 회원국의 법정에서 진행되어야 한다.

#### GDPR 관련 규정

- 제77조(감독기구에 민원을 제기할 권리)
- 제78조(감독기구에 대한 유효한 사법 구제권)
- 제79조(컨트롤러 또는 프로세서 대상 유효한 사법 구제권)

#### 개인정보보호법 관련 규정

- 제62조(침해 사실의 신고 등)

## 2

# 손해배상권 및 책임

## (Right to compensation and liability)

### (제82조)

#### Point

- 컨트롤러와 프로세서의 손해배상 의무를 이해할 수 있다.

#### 2.1 컨트롤러와 프로세서의 손해배상 의무

GDPR 규정 위반으로 물질적 또는 비물질적 피해를 입은 자는 누구든지 컨트롤러 또는 프로세서에게 손해배상을 받을 권리가 있다.

이를 구체적으로 살펴보면 다음과 같다.

- ① 개인정보 처리에 관여하는 컨트롤러는 위법한 정보 처리로 인해 발생한 피해에 대하여 책임을 부담한다.

※ GDPR은 금전 및 비금전 손실에 대해서도 보상받을 수 있다는 점에서 *Directive* (손해배상권만 언급)와 차이가 있다.

- ② 프로세서 자신 또는 서브프로세서의 개인정보 처리와 관련하여 GDPR에 명시된 의무의 위반 또는 컨트롤러의 지시 사항 위반으로 발생한 손해에 대하여 책임을 부담한다.
- ③ 동일한(하나의) 개인정보 처리에 복수의 컨트롤러 또는 프로세서가 관여하여 손해가 발생한 경우, 이에 관여한 모든 당사자는 발생한 손해 전체에 대하여 책임을

부담한다.

※ 특정 손해에 대하여 공동 컨트롤러가 책임을 부담하는 상황에서 그 중 하나의 컨트롤러가 전체 손해액을 배상한 경우, 그는 다른 컨트롤러에 대하여 구상권 행사가 가능하다.

## 2.2 프로세서의 손해배상 의무

프로세서는 다음 경우에 한하여 발생한 손해에 대하여 책임을 부담한다.

- ① GDPR에서 규정한 프로세서의 의무를 준수하지 않은 경우
- ② 컨트롤러의 합법적인 지시에 반하여 행위한 경우
- ③ 컨트롤러의 합법적인 지시의 범위를 벗어나 행위한 경우

## 2.3 책임 면제

책임 부담의 일반 원칙에 따라, 컨트롤러나 프로세서가 손해를 일으킨 사건에 대하여 책임이 없음을 증명하면 해당 책임으로부터 면제된다.

### GDPR 관련 규정

- 제82조(손해배상권 및 책임)

### 개인정보보호법 관련 규정

- 제39조(손해배상 책임)



# 3

## 과징금 (Administrative fines)

### (제83조)

#### Point

- 과징금 부과 및 가액의 원칙을 이해할 수 있다.

#### 3.1 원칙

과징금은 자동으로 적용되지 않으며, 개별 사례별(each individual case)로 부과된다.

※ 과징금이 부과되는 위반 행위는 매우 다양하며, 감독기구는 과징금의 부과 여부 및 과징금 가액을 결정할 때 GDPR 제83조에 명시된 개별 사안별로 평가한다.

과징금의 부과는 효과적이고 비례적이며, 설득력이 있어야 한다.

동일하거나 관련된 처리가 GDPR의 여러 규정 위반을 수반할 경우, 과징금은 가장 중한 침해에 지정되는 액수를 초과할 수 없다.

#### 3.2 최대 과징금

##### 3.2.1. 전세계 연간 매출액 4% 또는 2천만 유로 중 더 큰 금액

GDPR 규정을 심각하게 위반하는 경우(serious infringements) 직전 회계연도 전세계 매출액의 4% 또는 2천만 유로 중 더 큰 금액의 과징금이 부과된다.

여기에서 '심각한 위반'은 다음 경우를 의미한다.

- ① '동의'를 비롯한 개인정보 처리의 기본 원칙을 위반한 경우(제5~7조 및 제9조 위반)
- ② 정보주체의 권리를 보장하지 않는 경우(제12~22조 위반)
- ③ 제3국이나 국제기구의 수령인에게로 개인정보를 이전할 때 준수해야 할 규정을 위반한 경우(제44~49조 위반)
- ④ 제24~43조에 따라 채택된 회원국 법률에 따른 의무를 위반한 경우
- ⑤ 제58조제2항에 따라 감독기구가 내린 명령 또는 정보 처리의 임시적 또는 확정적 제한(temporary or definitive limitation)에 불복하는 경우, 또는 개인정보 이동 중지 명령을 준수하지 않거나 정보주체의 열람권을 보장하지 않아 제58조제1항을 위반한 경우

※ 제58조에 명시된 감독기구의 시정 권한에 따른 명령을 불복하는 경우 2천만 유로에 이르는 과징금이 부과될 수 있다.

### 3.2.2 전세계 연간 매출액 2% 또는 1천만 유로 중 더 큰 금액

다음 경우에는 1천만 유로 또는 직전 회계연도의 연간 전세계 총 매출의 2%에 이르는 과징금 중 더 큰 금액의 처분을 받게 된다.

- ① 컨트롤러, 프로세서의 의무를 위반한 경우(제8조, 제11조, 제25~39조, 제42조, 제43조 위반)
- ② 인증기관의 의무를 위반한 경우(제42조, 제43조 위반)
- ③ 행동규약 준수 모니터링의 의무를 위반한 경우(제41조제4항 위반)

#### GDPR 관련 규정

- 제83조(과징금 부과에 관한 일반 조건)

#### 개인정보보호법 관련 규정

- 제34조의2(과징금의 부과 등)

## 4 벌칙 (Penalties) (제84조)

개별 EU 회원국의 법률상 차이로 인해 서로 다른 수준의 벌칙이 존재할 것으로 예상된다. 특히 GDPR을 위반하였을 때 개별 회원국이 사법 제재(criminal sanctions)를 규정할 수 있어 컨트롤러 또는 프로세서에게 직접적인 벌칙이 이루어질 수도 있다.

개별 EU 회원국은 GDPR에 따라 각국 법률에 반영하는 조치를 2018년 5월 25일까지 EU 집행위원회에 통보하여야 한다.

### GDPR 관련 규정

- 제84조(벌칙)

### 개인정보보호법 관련 규정

- 제9장(벌칙)

## 더 알아보기 10

## 과징금 부과 및 가액 평가 기준

감독기구는 과징금 부과 및 가액을 평가할 때 개별 사안별 모든 정황을 고려하여야 하며, 이 때 제83조에 명시된 부과 및 가액 결정에 대한 조문뿐 아니라, 제58조제2항에 따른 시정 조치, 전문 제148항에 따른 징계 등 다양한 제재 방안을 고려하여야 합니다.

## #1 위반 행위의 성격, 심각성 및 지속 기간

## 위반 행위의 성격

위반 행위의 성격에 따라 최대 과징금은 서로 다르게 규정됩니다. 감독기구는 제83조제2항에 규정된 기준을 고려하여 과징금 부과 수준을 결정할 수 있는데, 이 때 최대 과징금이 높은 규정에 명시된 위반 행위가 상대적으로 낮은 규정의 위반 행위보다 반드시 높은 과징금을 부과 받는 것은 아닙니다.

또한 경미한 위반의 경우 또는 컨트롤러가 개인이고 과징금이 부담이 되는 경우 구체적인 평가를 통하여 전문 제148항에 따른 징계로 대체될 수 있습니다.

## 위반 행위의 심각성 및 지속 기간

GDPR은 위반 행위별 상세 과징금 부과 금액을 규정하고 있지 않고 있습니다. 다만 최대 금액에 대한 규정을 통하여 최대 과징금 부과 금액이 상대적으로 낮은 조항의 위반 행위인 경우 그 심각성(gravity)이 낮은 것으로 볼 수도 있습니다. 또한 위반의 성격, 정보주체의 수, 개인정보 처리의 범위와 목적, 피해 수준, 위반 행위의 지속 기간 등도 심각성 평가의 요소로 볼 수 있습니다.

## ① 정보주체의 수

위반 행위로 인해 영향을 받는 정보주체의 수로, 데이터베이스에 저장된 총 건수, 서비스 이용자의 수, 고객의 수 또는 국가 총 인구수 등이 해당합니다.

## ② 목적

명시된 정보 처리의 목적과 그 목적에 따른 적합한 처리 여부의 측면에서 개인정보 처리 작업을 평가하고, 위반 행위의 심각성을 평가하여야 합니다.

## ③ 피해 수준

전문 제74항에 따라 개인정보의 처리 결과가 개인에게 다양한 신체적·물질적·정신적 피해를 유발할 수 있는 경우에는 위반 행위의 심각성을 고려할 수 있습니다.

## ④ 지속 기간

위반 행위의 지속 기간은 심각성 평가의 주요 고려 사항입니다. 지속 기간에 따라 컨트롤러의 의도적 위반 행위, 적절한 예방 조치의 미실시, 필수적인 기술적·관리적 조치 시행 역량의 부재 여부 등을 판단할 수도 있습니다.

# #2 위반의 의도성 또는 태만

의도성(intent)이란 위반 행위에 대한 지식과 고의성을 의미합니다. 비의도적(unintentional) 위반은 법규 의무를 위반하였으나 위반을 유발할 의도가 없었음을 의미합니다.

의도적 위반은 비의도적 위반보다 심각하게 받아들여지므로 과징금 부과 가능성 또한 높습니다. 의도적 위반 행위는 최고 경영진의 승인에 따른 불법적 개인정보 처리 또는 DPO의 의견을 무시한 개인정보 처리 등이 해당됩니다.

태만 행위는 현행 정책 미준수, 인적 오류(human error), 공개 정보 내 개인정보 포함 여부 미확인, 적정 시점의 기술적 업데이트 실패, (단순 정책 미적용이 아닌) 정책 자체의 미수립 등이 해당됩니다.

# #3 정보주체의 피해를 경감하기 위한 조치

컨트롤러와 프로세서는 규정 위반 행위로 인해 정보주체에게 피해가 발생한 경우,

책임 있는 당사자로서 해당 개인에 대한 부정적 영향을 줄이기 위하여 가능한 모든 수단을 동원하여야 합니다.

※ 예 : 데이터 처리와 관련된 다른 컨트롤러·프로세서에게 연락, 이미 발생한 것 보다 심각한 영향을 미칠 수 있는 수준 또는 단계로 피해 확대를 중단시키기 위한 조치 등

#### #4 적절한 기술적·관리적 보호조치의 고려 여부

감독기구는 위반 행위가 발생한 개인정보 처리에 대하여 ① 제25조에 따른 data protection by design and by default의 원칙을 고려하였는지, ② 제32조에 따른 적정 수준의 보안 조치를 실행하였는지, ③ 제24조에 따른 기술적·관리적 조치의 준수와 공인된 행동규약 및 인증 메커니즘을 고려하였는지 등을 통하여 적정 수준의 보호조치 여부를 평가할 수 있습니다.

#### #5 과거 위반 행위 확인 및 조치 여부

감독기구는 ① 컨트롤러·프로세서의 동일 위반 행위 발생 여부, ② 컨트롤러·프로세서의 동일 방식의 규정 위반 행위 발생 여부 확인을 통하여 현재 개인정보 처리 위반 행위의 관련성을 평가할 수 있습니다.

#### #6 위반 행위 개선을 위한 감독기구와의 협조

GDPR 제83조제2항은 과징금 부과 여부 및 과징금 가액 결정시 컨트롤러·프로세서의 협조 수준에 따라 상당한 고려가 이루어질 수 있다고 규정하고 있습니다.

#### #7 위반으로 인해 영향을 받게 되는 개인정보의 종류

위반 행위를 통하여 영향을 받는 개인정보가 다음에 해당하는지 여부에 따라 과징금 가액 결정은 상이할 수 있습니다. ① 민감정보 또는 범죄경력 및 범죄행위 관련 정보인

경우, ② 처리되는 정보가 직접 또는 간접적으로 식별 가능한 경우, ③ 처리되는 정보의 유출이 개인에게 즉각적인 피해와 고통을 야기할 경우, ④ 개인정보 접근통제를 위한 기술적 보호조치가 적용된 경우

## **#8 감독기구에 위반 행위 발생 사실 통지 여부**

컨트롤러의 위반 행위에 대한 감독기구 통지는 법적 의무이므로 그 이행에 따라 처벌 수준이 경감될 수는 없습니다. 다만 그 의무를 미이행한 컨트롤러·프로세서는 보다 중대한 제재 대상으로 판단될 수 있습니다.

## **#9 과거 동일한 사안에 대한 감독기구의 시정 조치 내역**

감독기구는 동일 위반 행위 발생 시 컨트롤러·프로세서의 과거 조치 내역을 참조하여 과징금 부과 여부 및 과징금 결정 가액 등을 결정하게 되므로 과거 사례는 현재 위반 행위의 평가에 있어 참조 기준이 될 수 있습니다.

## **#10 승인된 행동규약 및 인증 메커니즘의 준수 여부**

감독기구는 제57조제1항(a)에 따른 GDPR의 감시 및 집행 의무의 이행을 위하여 컨트롤러·프로세서에게 승인된 행동규약을 준수하도록 할 수 있습니다. 이때 컨트롤러와 프로세서는 모니터링 기구에 의해 행동규약의 준수 여부가 감시되며, 이러한 메커니즘을 통하여 감독기구는 추가 조치 필요 여부를 판단 할 수 있습니다.

## **#11 위반으로 인해 직·간접적으로 얻은 금전적 이익 또는 회피한 손실**

위반 행위를 통하여 얻은 이익에 대한 정보는 과징금 부과에 강력한 근거가 될 수 있습니다. 따라서 기업이 위반 행위를 통하여 얻은 직·간접적 이익이나 회피한 손실 등을 검토하는 것은 중요합니다.

## 더 알아보기 11

## GDPR의 제재 규정

제재 종류	주요 내용	관련 조문	
손해배상 (제82조)	• GDPR 위반의 결과로 물질적 또는 비물질적 손해를 입은 정보주체는 그 손해에 대하여 컨트롤러나 프로세서로부터 배상을 받을 수 있다.	-	
	• 컨트롤러는 GDPR을 위반하는 처리가 일으킨 손해에 대하여 책임을 져야 한다.		
	• 다만 손해를 일으킨 사건에 대하여 책임이 없음을 입증하면, 컨트롤러 또는 프로세서의 책임 면제가 가능하다.		
과징금 (제83조)	• 복수의 컨트롤러 또는 프로세서가 일으킨 손해에 대하여 책임이 있는 경우 정보주체의 실질적 배상을 위하여 모든 손해에 대한 책임을 부담한다.	-	
	• 이 경우 하나의 컨트롤러나 프로세서가 완전한 배상을 하면 다른 컨트롤러나 프로세서에 대한 구상권 행사가 가능하다.		
	• EU 회원국 감독기구는 과징금 부과 권한이 있다.		
과징금 (제83조)	• EU 회원국의 법체계에 과징금 부과 근거가 없는 경우, 회원국의 법원이 해당 과징금을 부과할 수도 있다.	-	
	• 컨트롤러나 프로세서가 고의 또는 과실로 GDPR의 여러 규정을 위반한다면, 과징금 총액은 가장 중한 위반에 규정된 금액을 초과하여서는 안 된다.		
	전세계 연간 매출액 2% 또는 1천만 유로 중 더 큰 금액 부과		
	• 컨트롤러 및 프로세서 의무 위반		제8조, 제11조, 제25~39조, 제42조, 제43조
	• 인증기관 의무 위반		제42조, 제43조
• 공인된 행동규약 준수에 대한 모니터링 의무 위반	제41조제4항		
전세계 연간 매출액 4% 또는 2천만 유로 중 더 큰 금액 부과			
벌칙 (제84조)	• 동의를 조건을 포함하여 개인정보 처리 기본 원칙 위반	-	
	• 정보주체의 권리 보장 의무 위반		제5~7조, 제9조
	• 제3국이나 국제기구의 수령인에게 개인정보 이전 시 준수 의무 위반		제12~22조
	• 제24~43조에 따라 채택된 EU 회원국 법률 의무 위반		제44~49조
	• 감독기구가 내린 명령 또는 정보 처리의 제한 불복		제58조제2항
• 감독기구의 개인정보 이동 중지 명령 미준수 및 정보주체의 열람권 보장 의무 위반	제58조제1항		
벌칙 (제84조)	• 회원국의 과징금이 부과되지 않는 위반에 대한 벌칙 규정 신설 의무(제1항)	-	
	• 각 회원국은 제1항에 따라 채택하는 법 규정을 2018년 5월 25일까지, 그리고 해당 법 규정에 영향을 미치는 후속 개정을 지체 없이 유럽 집행위원회에 통보하여야 한다.		

## IX

## 피해 구제 및 제재 규정





## X. 참고 자료

---

1. GDPR 적용 대상 국가의 감독기구 현황
2. 주요 질의 및 답변(Q&A)
3. 사업자를 위한 EU 집행위원회의 7단계 체크리스트

# 1. GDPR 적용 대상 국가의 감독기구 현황

## EU 국가별 감독기구 현황

(2018년 4월 19일 현재)

### 오스트리아(Austria)

**Österreichische Datenschutzbehörde**  
Wickenburggasse 8  
1080 Wien  
Tel. +43 1 52152-0  
e-mail: dsb@dsb.gv.at  
Website: <http://www.dsb.gv.at/>

### 벨기에(Belgium)

**Commission de la protection de la vie privée**  
**Commissie voor de bescherming van de persoonlijke levenssfeer**  
Rue de la Presse 35 / Drukpersstraat 35  
1000 Bruxelles / 1000 Brussel  
Tel. +32 2 274 48 00  
Fax +32 2 274 48 35  
e-mail: [commission@privacycommission.be](mailto:commission@privacycommission.be)  
Website: <http://www.privacycommission.be/>

### 불가리아(Bulgaria)

**Commission for Personal Data Protection**  
2, Prof. Tsvetan Lazarov blvd.  
Sofia 1592  
Tel. +359 2 915 3580  
Fax +359 2 915 3525  
e-mail: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)  
Website: <http://www.cdpd.bg/>

### 크로아티아(Croatia)

**Croatian Personal Data Protection Agency**  
Martićeva 14  
10000 Zagreb  
Tel. +385 1 4609 000  
Fax +385 1 4609 099  
e-mail: [azop@azop.hr](mailto:azop@azop.hr) or [info@azop.hr](mailto:info@azop.hr)  
Website: <http://www.azop.hr/>

### 키프로스(Cyprus)

**Commissioner for Personal Data Protection**  
1 Iasonos Street,  
1082 Nicosia  
P.O. Box 23378, CY-1682 Nicosia  
Tel. +357 22 818 456  
Fax +357 22 304 565  
e-mail: [commissioner@dataprotection.gov.cy](mailto:commissioner@dataprotection.gov.cy)  
Website: <http://www.dataprotection.gov.cy/>

### 체코(Czech Republic)

**The Office for Personal Data Protection**  
Urząd pro ochranu osobních údajů  
Pplk. Sochora 27  
170 00 Prague 7  
Tel. +420 234 665 111  
Fax +420 234 665 444  
e-mail: [posta@uouu.cz](mailto:posta@uouu.cz)  
Website: <http://www.uouu.cz/>

**덴마크(Denmark)****Datatilsynet**

Borgergade 28, 5  
1300 Copenhagen K  
Tel. +45 33 1932 00  
Fax +45 33 19 32 18  
e-mail: dt@datatilsynet.dk  
Website: <http://www.datatilsynet.dk/>

**에스토니아(Estonia)****Estonian Data Protection Inspectorate  
(Andmekaitse Inspektsioon)**

Väike-Ameerika 19  
10129 Tallinn  
Tel. +372 6274 135  
Fax +372 6274 137  
e-mail: info@aki.ee  
Website: <http://www.aki.ee/en>

**핀란드(Finland)****Office of the Data Protection  
Ombudsman**

P.O. Box 315  
FIN-00181 Helsinki  
Tel. +358 10 3666 700  
Fax +358 10 3666 735  
e-mail: tietosuoja@om.fi  
Website: <http://www.tietosuoja.fi/en/>

**프랑스(France)****Commission Nationale de l'Informatique  
et des Libertés - CNIL**

8 rue Vivienne, CS 30223  
F-75002 Paris, Cedex 02  
Tel. +33 1 53 73 22 22  
Fax +33 1 53 73 22 00  
Website: <http://www.cnil.fr/>

**독일(Germany)****Die Bundesbeauftragte für den  
Datenschutz und die Informationsfreiheit**

Husarenstraße 30  
53117 Bonn  
Tel. +49 228 997799 0, +49 228 81995 0  
Fax +49 228 997799 550  
+49 228 81995 550  
e-mail: poststelle@bfdi.bund.de  
Website: <http://www.bfdi.bund.de/>

**그리스(Greece)****Hellenic Data Protection Authority**

Kifisias Av. 1-3, PC 11523  
Ampelokipi Athens  
Tel. +30 210 6475 600  
Fax +30 210 6475 628  
e-mail: contact@dpa.gr  
Website: <http://www.dpa.gr/>

**헝가리(Hungary)****National Authority for Data Protection  
and Freedom of Information**

Szilágyi Erzsébet fasor 22/C  
H-1125 Budapest  
Tel. +36 1 3911 400  
e-mail: peterfalvi.attila@naih.hu  
Website: <http://www.naih.hu/>

**아일랜드(Ireland)**

Data Protection Commissioner  
Canal House  
Station Road  
Portarlington  
Co. Laois  
Lo-Call: 1890 25 22 31  
Tel. +353 57 868 4800  
Fax +353 57 868 4757  
e-mail: info@dataprotection.ie  
Website: <http://www.dataprotection.ie/>

## 이탈리아(Italy)

### **Garante per la protezione dei dati personali**

Piazza di Monte Citorio, 121  
00186 Roma  
Tel. +39 06 69677 1  
Fax +39 06 69677 785  
e-mail: [garante@garanteprivacy.it](mailto:garante@garanteprivacy.it)  
Website: <http://www.garanteprivacy.it/>

## 라트비아(Latvia)

### **Data State Inspectorate**

**Director:** Ms Daiga Avdejanova  
Blaumana str. 11/13-15  
1011 Riga  
Tel. +371 6722 3131  
Fax +371 6722 3556  
e-mail: [info@dvi.gov.lv](mailto:info@dvi.gov.lv)  
Website: <http://www.dvi.gov.lv/>

## 리투아니아(Lithuania)

### **State Data Protection**

Žygimantų str. 11-6a  
011042 Vilnius  
Tel. + 370 5 279 14 45  
Fax +370 5 261 94 94  
e-mail: [ada@ada.lt](mailto:ada@ada.lt)  
Website: <http://www.ada.lt/>

## 룩셈부르크(Luxembourg)

### **Commission Nationale pour la Protection des Données**

1, avenue du Rock'n'Roll  
L-4361 Esch-sur-Alzette  
Tel. +352 2610 60 1  
Fax +352 2610 60 29  
e-mail: [info@cnpd.lu](mailto:info@cnpd.lu)  
Website: <http://www.cnpd.lu/>

## 몰타(Malta)

### **Office of the Data Protection Commissioner**

Data Protection Commissioner: Mr Joseph Ebejer  
2, Airways House  
High Street, Sliema SLM 1549  
Tel. +356 2328 7100  
Fax +356 2328 7198  
e-mail: [commissioner.dataprotection@gov.mt](mailto:commissioner.dataprotection@gov.mt)  
Website: <http://www.dataprotection.gov.mt/>

## 네덜란드(Netherlands)

Autoriteit Persoonsgegevens  
Prins Clauslaan 60  
P.O. Box 93374  
2509 AJ Den Haag/The Hague  
Tel. +31 70 888 8500  
Fax +31 70 888 8501  
e-mail: [info@autoriteitpersoonsgegevens.nl](mailto:info@autoriteitpersoonsgegevens.nl)  
Website: <https://autoriteitpersoonsgegevens.nl/nl>

## 폴란드(Poland)

### **The Bureau of the Inspector General for the Protection of Personal Data - GIODO**

ul. Stawki 2  
00-193 Warsaw  
Tel. +48 22 53 10 440  
Fax +48 22 53 10 441  
e-mail: [kancelaria@giodo.gov.pl](mailto:kancelaria@giodo.gov.pl)  
[desiwm@giodo.gov.pl](mailto:desiwm@giodo.gov.pl)  
Website: <http://www.giodo.gov.pl/>

**포르투갈(Portugal)****Comissão Nacional de Protecção de Dados - CNPD**

R. de São. Bento, 148-3°  
 1200-821 Lisboa  
 Tel. +351 21 392 84 00  
 Fax +351 21 397 68 32  
 e-mail: geral@cnpd.pt  
 Website: <http://www.cnpd.pt/>

**루마니아(Romania)**

The National Supervisory Authority for  
 Personal Data Processing  
 President: Mrs Ancuța Gianina Opre  
 B-dul Magheru 28-30  
 Sector 1, BUCUREȘTI  
 Tel. +40 21 252 5599  
 Fax +40 21 252 5757  
 e-mail: [anspdc@dataprotection.ro](mailto:anspdc@dataprotection.ro)  
 Website: <http://www.dataprotection.ro/>

**슬로바키아(Slovakia)**

Office for Personal Data Protection of the  
 Slovak Republic  
 Hraničná 12  
 820 07 Bratislava 27  
 Tel.: + 421 2 32 31 32 14  
 Fax: + 421 2 32 31 32 34  
 e-mail: [statny.dozor@pdp.gov.sk](mailto:statny.dozor@pdp.gov.sk)  
 Website: <http://www.dataprotection.gov.sk/>

**슬로베니아(Slovenia)**

Information Commissioner  
 Ms Mojca Prelesnik  
 Zaloška 59 1000 Ljubljana  
 Tel. +386 1 230 9730  
 Fax +386 1 230 9778  
 e-mail: [gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)  
 Website: <https://www.ip-rs.si/>

**스페인(Spain)****Agencia de Protección de Datos**

C/Jorge Juan, 6  
 28001 Madrid  
 Tel. +34 91399 6200  
 Fax +34 91455 5699  
 e-mail: [internacional@agpd.es](mailto:internacional@agpd.es)  
 Website: <https://www.agpd.es/>

**스웨덴(Sweden)****Datainspektionen**

Drottninggatan 29  
 5th Floor  
 Box 8114  
 104 20 Stockholm  
 Tel. +46 8 657 6186  
 Fax +46 8 652 8652  
 e-mail: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)  
 e-mail: [lena.schelin@datainspektionen.se](mailto:lena.schelin@datainspektionen.se)  
 Website: <http://www.datainspektionen.se/>

**영국(United Kingdom)**

The Information Commissioner's Office  
 Water Lane, Wycliffe House  
 Wilmslow - Cheshire SK9 5AF  
 Tel. +44 1625 545 745  
 e-mail: [international.team@ico.org.uk](mailto:international.team@ico.org.uk)  
 Website: <https://ico.org.uk>

## 유럽 자유무역 연합(EUROPEAN FREE TRADE AREA)

### 아이슬란드(Iceland)

Icelandic Data Protection Agency  
Rauðarárstíg 10  
105 Reykjavík  
Tel. +354 510 9600  
Fax +354 510 9606  
e-mail: postur@personuvernd.is

### 리히텐슈타인(Liechtenstein)

Data Protection Office  
Kirchstrasse 8, P.O. Box 684  
9490 Vaduz  
Principality of Liechtenstein  
Tel. +423 236 6090  
e-mail: info.dss@lv.li

### 노르웨이(Norway)

Datatilsynet  
The Data Inspectorate  
P.O. Box 8177 Dep  
0034 Oslo  
Tel. +47 22 39 69 00  
Fax +47 22 42 23 50  
e-mail: postkasse@datatilsynet.no

### 스위스(Switzerland)

Data Protection and Information  
Commissioner of Switzerland  
Eidgenössischer Datenschutz- und  
Öffentlichkeitsbeauftragter  
**Mr Adrian Lobsiger**  
Feldegweg 1 3003 Bern  
Tel. +41 58 462 43 95  
Fax +41 58 462 99 96  
e-mail: contact20@edoeb.admin.ch

## 2. 주요 질의 및 답변(Q&A)

아래 질문과 답변은 EU 집행위원회에서 공개 게시한 FAQs와 한국인터넷진흥원 국제협력센터를 통하여 접수된 질의를 바탕으로 구성되었습니다. 아래의 질의응답 사례는 GDPR 전체의 내용을 포괄하지 않을 수 있으며, GDPR 본격 시행 이후 EC의 입장과 실제 판결 사례와 상황에 따라 그 내용이 변경될 수 있으므로 해당 자료에만 의존한 의사결정에 대하여 권장하지 않습니다.

또한 본 질의응답을 바탕으로 한 의사결정의 책임은 한국인터넷진흥원에 있지 않음을 알려 드립니다.

### EU 집행위원회 질의응답 사례



#### 1. GDPR에서 정의하는 개인정보란 무엇인가요?



#### A GDPR에서 정의하는 개인정보란,

식별되거나 식별 가능한 정보주체(자연인)와 관련된 모든 정보를 의미하며, 다른 정보와의 결합을 통하여 개인을 식별할 수 있는 정보도 개인정보로 정의하고 있습니다.

예) 성명, 주소, 이메일 주소, 신분증 번호, 위치 정보, IP 주소, 쿠키 ID, 휴대전화의 식별정보, 병원이나 의사가 보유한 정보 중 개인을 식별할 수 있는 정보.

가명정보는 재식별이 가능하기 때문에 개인정보로 분류되며, 익명정보는 개인정보로 보지 않습니다.



#### 2. 개인정보 처리 (Processing)는 어떤 행위를 포함하나요?



#### A 개인정보 처리는,

개인정보의 수집, 저장, 변경, 삭제, 공개, 전송, 결합 등을 포괄합니다.

예) ① 임직원 관리 및 급여 관리 ② 광고성 메일 발송 ③ 개인정보를 포함하고 있는 연락처에 대한 접근 및 조회 ④ 개인정보를 포함하고 있는 문서의 파쇄 ⑤ 개인의 사진을 온라인에 게시 ⑥ IP 주소 및 MAC 주소의 저장 ⑦ 동영상 녹화(CCTV)



#### 3. GDPR의 적용 범위는 어떻게 되나요?



#### A GDPR의 적용 범위는 크게 다음의 두 가지로 구분될 수 있습니다.

- 1) EU 내에 설립된 기업이 개인정보를 처리하는 경우
- 2) EU 외부에 설립된 기업이 EU 역내에 재화나 서비스를 제공



하거나 EU 역내의 정보주체를 모니터링하는 경우

예) ① GDPR 적용 경우 : 교육 업체가 EU 내의 스페인권과 포르투갈어권 대학에 강자를 개설하고, 서비스 제공을 위하여 고객의 ID와 비밀번호를 요구하는 경우 ② GDPR 적용 예외 경우 : EU 역외에 설립된 기업이 EU 역내의 정보주체를 구체적으로 겨냥하지 않은 상황에서, EU 내 정보주체가 서비스를 활용하는 경우

#### 4. 컨트롤러(Controller)와 프로세서(Processor)란 무엇인가요?

##### 컨트롤러와 프로세서는 '개인정보 처리'의 주체입니다.

컨트롤러는 개인정보 처리의 목적과 방법을 결정하는 주체를 의미하며, 이와 같은 결정권을 제3자와 공동으로 행사할 경우 공동 컨트롤러(Joint controller)의 지위를 획득합니다.  
프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 주체로, 프로세서의 책임과 의무는 양자 간의 서면 계약서에 명시되어야 합니다.

예) 한 기업이 급여 관리 대행사와 직원의 임금 관리 업무 계약을 맺고, 대행사가 IT 시스템을 구축하여 직원들의 정보를 처리하는 경우, 업무를 요청한 기업은 컨트롤러가 되고 급여 대행사는 프로세서가 됨

#### 5. 개인정보 삭제권(잊힐 권리)이란 무엇인가요?

##### 정보주체는 다음의 경우 본인의 개인정보에 대한 삭제를 요청할 수 있습니다.

1) 당초 수집 목적을 달성한 경우, 2) 동의를 철회한 경우, 3) 처리에 반대하는 경우, 4) 불법적인 처리의 경우, 5) 국가의 법적 의무 준수를 위한 경우, 6) 아동에게 제공할 정보사회서비스와 관련하여 개인 정보를 처리한 경우

예) ① 개인정보를 삭제하여야 하는 경우

- 정보주체가 SNS 서비스를 활용하다 탈퇴한 후 정보 삭제를 요청한 경우
- 정보 삭제에 의한 개인의 이익이 정보 공개에 의한 공익을 능가하는 경우(검색 엔진에서 개인 정보가 담긴 링크나 웹 페이지 삭제)

② 즉시 삭제를 할 수 없는 경우

- 다른 개별법에서 개인정보의 보관을 명문화한 경우(이 경우, 정보주체는 자신의 정보에 대한 처리의 제한을 요구할 수 있음)

## Q 6. 개인정보 이동권이란 무엇인가요?

**A** 정보주체는 다음에 해당하는 자신의 정보를 다른 기업에 전송할 것을 요청할 수 있습니다.

- 1) 정보주체가 컨트롤러에게 제공하였으며, 2) 정보주체의 동의에 근거하거나 계약의 이행을 위해, 3) 처리가 자동화된 수단에 의해 이루어지는 경우

예) SNS 서비스 고객이 타 SNS 서비스로 사진 등의 개인정보 이동을 요청한 경우

## Q 7. DPO(Data Protection Officer)란 무엇이며 어떤 경우 필수로 지정해야 하나요?

**A** DPO는,

컨트롤러·프로세서의 개인정보 처리 활동 전반에 관해 자문 역할을 하는 전문가로, 조직의 관리 체계 구축·임직원 교육·감독기구와의 의사소통 등의 역할을 수행합니다.

기업은 DPO로 조직 내부의 직원을 임명할 수 있으며, 외부 서비스 계약에 의한 DPO 임명도 고려할 수 있습니다. 또한 DPO는 기업으로부터 업무상 지시를 받지 않으며, 최고 경영진에게 직접 보고할 수 있는 권한이 보장되어야 합니다.

다음의 경우에 컨트롤러·프로세서는 DPO를 필수로 지정하여야 합니다.

- 1) 기업의 핵심 활동이 대규모 민감정보 처리를 포함하는 경우
- 2) 기업의 핵심 활동이 개인에 대한 대규모의 정기적이고 체계적인 모니터링을 포함하는 경우
- 3) 정부부처 및 관련기관의 경우(법원 제외)

예) ① DPO를 필수로 지정하여야 하는 경우

- 민감정보를 대규모로 처리하는 병원
- 쇼핑물이나 공공장소를 모니터링 하는 보안 회사
- 개인의 프로필을 축적하는 헤드헌팅 업체

② DPO를 임명하지 않아도 되는 경우

- 환자의 정보를 처리하는 의사 개인
- 고객의 정보를 처리하는 소규모 법무 법인

## Q 8. 개인정보 영향평가는 어떤 경우 요구되나요?

**A** 개인정보 영향평가는,

개인정보 처리가 정보주체의 자유와 권리에 높은 위험을 초래할 가능성이 있는 경우 수행되어야 하며,

영향평가가 특히 요구되는 경우는 다음과 같습니다.

- 1) 처리가 정보주체의 개인적 측면에 대한 체계적이고 광범위한 평가인 경우
- 2) 대규모 민감 정보를 처리하는 경우
- 3) 공공장소에 대한 체계적인 대규모의 모니터링에 해당하는 경우

개인정보 영향평가는 처리 이전 단계에서 수행되어야 하며, 해당 조치를 통해서도 완화될 수 없는 위험이 있는 경우에는 감독기구와 협의가 필요합니다.

예) ① 영향평가가 필요한 경우

- 은행이 신용 정보를 활용하여 고객을 검열하는 경우
- 병원에서 환자의 건강 정보를 포함하여 새로운 건강 정보 데이터 베이스를 구축하려는 경우
- 버스 회사가 기사와 승객의 행동을 감시하기 위하여 차내 카메라를 설치하는 경우 등

② 영향평가가 불필요한 경우

- 의사가 한정된 숫자의 환자의 개인정보를 처리하는 경우에는 해당 처리가 대규모로 이루어지지 않기 때문에 영향평가가 불필요

## 9. 개인정보를 역외 이전할 수 있는 조건은 무엇인가요?


 EU 역내에서 수집한 개인정보는 다음의 경우 EU 역외로 이전 가능합니다.

- 1) EU 집행위원회로부터 적정성 승인(Adequacy Decision)을 받은 경우
- 2) 적정성 승인을 받지 않았지만, 다음의 보호조치를 마련한 경우
  - ① 구속력 있는 기업 규칙 (Binding Corporate Rules, BCRs)
  - ② 표준 개인정보보호 조항(Standard data protection clauses)에 의거한 개인정보 이전 계약
  - ③ 승인된 행동규약(code of conduct) 및 인증제도 (certification)
- 3) 정보주체가 명시적으로 동의한 경우

예) EU 역외(우루과이, 아르헨티나, 브라질)로 개인정보를 이전하는 경우 중

- 우루과이와 아르헨티나는 적정성 승인을 받았기 때문에, 별도의 보호 조치 없이 개인정보의 이전이 가능
- 브라질은 적정성 승인을 받지 않았기 때문에 위의 3가지 보호조치 중 하나를 채택한 경우 또는 정보주체의 명시적 동의가 있는 경우에만 역외 이전이 가능

## 10. GDPR 위반에 따른 과징금의 부과 및 가액 원칙은 무엇인가요?

 GDPR 위반의 경우 전세계 매출액 2% 또는 1천만 유로 중 더 큰 금액이, 심각한 위반의 경우 전세계 매출액 4% 또는 2천만 유로 중 더 큰 금액의 과징금이 부과됩니다.

과징금 산정에는 다음의 11가지 기준이 있으며, 침해 수준에 비례하여 과징금이 부과됩니다.

- 1) 위반의 성격, 중대성 및 지속 기간

- 2) 위반의 의도성 또는 태만 여부
- 3) 정보주체의 피해를 경감하기 위한 컨트롤러·프로세서의 조치
- 4) 기술적·조직적 보호조치를 고려한 컨트롤러·프로세서의 책임 수준
- 5) 컨트롤러·프로세서가 이전에 범했던 관련 법규의 위반 여부
- 6) 위반을 해결하기 위한 감독기구와의 협조 수준
- 7) 위반으로 인해 영향을 받게 되는 개인정보의 종류
- 8) 컨트롤러·프로세서의 위반 통지 여부
- 9) 동일한 사안에 대한 감독기구의 명령이 부과된 바가 있는지 여부
- 10) 승인된 행동 규약 또는 인증 메커니즘의 준수 여부
- 11) 위반으로 인해 직간접적으로 얻은 금전적 이익 또는 회피한 손실

## 한국인터넷진흥원 질의응답 사례



### 1. GDPR의 적용 범위

저희 쇼핑몰의 경우 전 세계적으로 재화를 판매하나 시스템과 운영은 한국에서 하고 있으며 다른 나라 사람에게 판매할 수 있는 영문 사이트도 운영을 하고 있습니다. 이에 유럽에 사는 사람들도 회원으로 가입을 하고 구매를 하는 경우가 있는데 이러한 경우에도 GDPR의 적용을 받아야 하나요?



GDPR은 기업이 '명백히' EU 시장을 염두에 두고 있을 때 적용됩니다. 여기서 '명백히'라고 함은, EU 시장에서 통용되는 언어나 통화를 직접적으로 제공하거나 그에 바탕을 두고 서비스를 제공함을 의미합니다.

한국에 있는 전자상거래 업체가 독일 도메인을 생성해 독일어로 홈페이지를 구성하고 있다면, 이는 독일 시장을 '명백히' 타겟팅하는 것으로 볼 수 있습니다.

반면 홈페이지를 영어로만 구성하고 통화도 달러만을 활용할 경우, GDPR의 직접적인 규제 대상에서 제외됩니다. EU 시민들의 단순 접근 가능성이 존재하지만, 전세계적으로 통용되는 영어와 달러화를 사용한 것이 EU 시장을 명백히 겨냥했다고 볼 수 없기 때문입니다.

다만 전자상거래 업체의 경우, 배송 서비스를 제공한다면 배송업체와 컨트롤러·프로세서 관계가 형성되면서 GDPR의 적용을 받을 여지가 있습니다.



### 2. 동의

GDPR은 '명시적 동의'에 근거해 민감정보의 처리 및 프로파일링, 개인정보의 역외 이전이 가능하다고 규정하고 있는데 '명시적' 동의의 정의는 무엇이며, 별도의 절차가 필요하지는 않나요?




'명시적'이란 정보주체에 의해 동의를 표현되는 방식을 의미합니다. 이는 일반적인 동의에 비해 정보주체의 동의를 명확하게 확인할 수 있는 방식을 의미합니다. 구체적으로, 이메일에 동의 의사를 표시하여 제출하거나, 전자서명을 하는 방식, 동의에 대한 2단계 검증 등이 명시적으로 동의를 표시하는 것으로 인정됩니다. 상황에 따라서는 예-아니오의 선택지와 함께 "나의 개인정보 처리에

동의합니다.(또는 동의하지 않습니다.)"와 같은 명확한 문구를 제시하는 것도 명시적 동의로 인정될 수 있습니다.

### 3. 컨트롤러와 프로세서

본사와 해외 법인과의 관계에서 누가 컨트롤러이고, 프로세서인가요?

 GDPR에 의하면 컨트롤러는 '개인정보의 처리 목적 및 수단을 결정하는 자연인 또는 법인 등'을 의미합니다. 즉 본사와 해외 법인 중, 현지에서 개인정보를 수집하는 목적과 수단을 규정하는 측이 컨트롤러라고 할 수 있습니다.


따라서 본사가 무조건 컨트롤러고 현지 법인이 프로세서라고 볼 수만은 없습니다.

개인정보 수집과 관련하여 본사가 해외 법인의 활동 범위를 규정한다면 본사가 컨트롤러가 될 것입니다.

반면, 본사의 특별한 지침이 없이 해외 법인이 자체적으로 개인정보의 수집 방식을 정한다면 해외 법인이 컨트롤러가 됩니다.

### 4. 자유와 권리에 높은 위험을 미치는 경우

GDPR은 개인의 자유와 권리에 '높은 위험'을 초래할 가능성이 있는 경우 다양한 보호조치 및 책임성 입증을 요구하고 있는데, GDPR에서 말하는 '높은 위험'이란 무엇이며 어떤 경우에 적용되나요?

 제29조 작업법에서 발간한 가이드라인에서 높은 위험을 초래할 가능성이 있는 개인정보 처리의 기준 9가지를 제시하고 있습니다.

해당 9가지 기준은 다음과 같습니다.

- 평가 또는 평점
- 법적 효과 또는 비슷한 다른 중요한 효과를 지닌 자동화된 의사 결정
- 시스템을 이용한 감시
- 민감정보
- 대규모 정보 처리
- 연계되거나 결합된 일련의 정보
- 취약한 정보주체(아동, 난민, 노인, 환자 등)에 관한 정보
- 신기술의 사용 (예 : 사물인터넷 관련 기술 적용)
- 처리 자체가 정보주체의 권리 행사나 서비스 이용 및 계약을 방해하는 경우

영향평가의 실시여부를 판단할 때, 원칙적으로 위의 9가지 유형 중 하나의 기준만을 충족하는 경우 위험수준이 낮기 때문에 영향평가를 필요로 하지 않을 수 있으나, 위의 기준 중 적어도 2개를 충족하는 처리작업은 DPIA가 필요하다고 할 수 있습니다.



## 5. DPO 지정

EU 내 법인이나 지사가 여러 곳이라면, 공동 DPO를 임명해도 되나요?



GDPR 제37조 제2항에 따라 사업체 그룹은 각 사업장에서 “쉽게 접근이 가능 경우(easily accessible)”, 복수 사업자가 단일 DPO를 지정할 수 있습니다.

단, ‘사업체 그룹(a group of undertakings)’에 해당하는 경우에만 가능하며, 사업적 관계가 없는 여러 독립 법인이 단일 DPO를 지정할 수는 없습니다.



## 6. 개인정보 처리 활동의 기록 의무

GDPR 준수와 관련한 처리 활동의 기록 의무 중, 종업원 수 250명 이하의 기업에서도 별도의 기록 및 문서화가 필요한 경우가 있나요?



컨트롤러와 프로세서는 GDPR 의무 준수 입증을 위해 개인정보 처리활동의 기록, 즉 문서화를 이행해야 합니다. GDPR에서는 영세 혹은 중소기업들의 상황을 고려해 종업원 수 250명 이상의 기업에 한해 개인정보 처리활동에 대한 기록을 의무적으로 문서화하도록 규정하고 있는데, 종업원수 250명 이하라도 정보주체의 권리와 자유에 위험을 초래할 가능성이 있는 개인정보, 민감 정보, 범죄 경력 및 범죄행위에 관련한 개인정보 처리 시에는 반드시 처리활동 기록이 필요합니다.



## 7. 개인정보 역외이전



개인정보 역외 이전에 대비하기 위한 대표적인 방법으로 구속력 있는 기업 규칙(BCRs)과 표준 개인정보보호 조항을 포함한 계약이 있는 것으로 알고 있는데, 각각의 장단점으로는 어떤 것이 있나요?

### 구속력 있는 기업 규칙(BCRs)

장점: 그룹 내부에서 일어나는 전체 개인정보 이전 활동에 대하여 보호조치를 적용할 수 있습니다.

단점: 규제 기관의 승인을 받는 데 시간이 소요될 수 있고, 그룹 외부로의 정보 이전에 대응할 수 없습니다.

### 표준 개인정보보호 조항(Standard data protection clauses)

장점: 승인된 계약을 통하여 개인정보 보호조치가 즉시 실행됩니다.

단점: 계약 당사자의 수가 많아질 경우 모든 상대방과 계약을 체결하기가 어려울 수 있고, 기업 구조 변경 등으로 계약 당사자가 변경되거나 이전하는 데이터 항목이 확대될 경우 이에 적합한 계약을 다시 체결해야 합니다. 정보 제공자(Data exporter)와 정보 수령인(Data importer)이 별도의 법인격으로 구분되지 않는 경우에는 계약을 체결하기 곤란하다는 점도 단점으로 꼽힙니다.



## 8. 개인정보 역외이전



표준 개인정보보호 조항을 포함한 계약을 체결할 때 정해진 양식이나 표준 양식이 있나요?  
계약서에는 어떤 항목이 필수적으로 들어가나요?

EU 집행위원회는 현재까지 아래와 같은 3가지 유형을 승인하고 있습니다.

### 〈컨트롤러에서 컨트롤러로 이전하는 경우〉

① Decision 2001 / 497 / EC : Set I

② Decision 2004 / 915 // EC : Set II

### 〈컨트롤러에서 프로세서로 이전하는 경우〉

③ Decision 2010 / 87 / EU (and repealing Decision 2002 / 16 / EC)

표준 개인정보보호 조항의 세부 내용은 EU 개인정보보호 원칙을 명시하고 있으며, 계약서의 유형과 관계없이 계약 당사자는 공통적으로 다음 내용을 작성하여야 합니다.

① 정보 제공자(Data exporter)와 정보 수령자(Data importer)의 연락처 등 기본 정보 ② 이전되는 정보 유형 및 민감정보, 범죄 경력 및 범죄 행위 관련 정보의 포함 여부 ③ 개인정보 처리의 목적 및 유형 등 표준 개인정보보호 조항의 내용은 계약 당사자 간 필요나 정보 처리 활동의 유형에 따라 변경될 수 있으나, 정보주체의 권리나 컨트롤러 및 프로세서의 의무를 준수하는 내용을 포함해야 합니다.

※ 현재까지 사용되고 있는 표준 개인정보보호 조항은 EC 홈페이지에서 확인할 수 있습니다.

([http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm))

### 3. 사업자를 위한 EU 집행위원회의 7단계 체크리스트<sup>41)</sup>

이 가이드는 GDPR에 대응하기 위해 중소기업 등이 짚고 넘어가야 할 7가지 단계의 체크리스트에 대해 기술하고 있습니다.

#### STEP 1

**수집 및 처리하는 개인정보를 확인하고, 수집·처리의 목적과 법적 근거를 검토 하였습니다니까?**



직원을 고용하는 경우 고용계약과 법적 의무 사항을 기반으로 개인정보를 수집하게 됩니다. 또한 고객의 개인정보를 수집하게 될 수도 있는데, 그 예로 마케팅 목적으로 동의 기반의 고객 정보를 수집할 수 있습니다. 공급업체와 비즈니스 고객의 개인정보를 수집하는 경우 계약에 근거하여야 하며, 계약이 반드시 서면일 필요는 없습니다.

#### STEP 2

**개인정보 수집 시 고객 및 직원 등 관련된 각 개인에게 관련된 정보를 전달하였습니까?**



개인정보 처리 대상인 개인은 어떤 목적으로 본인의 개인정보가 처리되는지 알고 있어야 합니다. 그러나, 배달음식을 주문하는 경우와 같이 고객이 이미 개인정보 처리와 관련된 세부 내용을 알고 있는 경우는 예외로 합니다. 만약 개인이 요청한 경우 개인정보를 열람할 수 있도록 해야 하고, 이 때 요청 정보를 가능한 한 신속하게 제공할 수 있도록 분류·보관하는 것이 권장됩니다.

41) EU 집행위원회(2018.), Seven steps for businesses to get ready for the General Data Protection Regulation



### STEP 3

#### 개인정보를 필요한 경우에만 보유하고 있습니까?



직원의 개인정보는 고용 관계 또는 법적 의무 사항 준수를 위한 경우에 한해 보유하여야 합니다.  
고객의 개인정보는 고객과의 관계 또는 법적 의무사항 준수를 위한 경우에 한해 보유하여야 합니다.  
즉, 개인정보는 당초 수집 목적에 따라 더 이상 필요하지 않다면 파기하여야 합니다.

### STEP 4

#### 처리하는 개인정보에 대하여 보호조치를 수립하였습니까?



IT 시스템에 개인정보를 보관하는 경우, 비밀번호 설정 등을 통하여 열람을 제한하여야 합니다.  
또한 이용하는 시스템의 보호조치가 정기적으로 최신성을 유지할 수 있도록 하여야 합니다. 만약 개인 정보를 물리적으로 보관하는 경우에는 비인가된 접근을 차단하고 안전한 장소에 보관하여야 합니다.

### STEP 5

#### 개인정보 처리 활동을 문서화하고 보유하고 있습니까?



처리하는 개인정보의 특성과 목적 등을 기록하여야 합니다. 감독기구의 요청에 적합하게 개인정보 처리를 기록할 필요가 있습니다. 문서화하여 기록하여야 하는 목록은 다음을 포함합니다.

- ① 개인정보 처리의 목적
- ② 개인정보의 유형
- ③ 정보주체의 범주
- ④ 수령인의 범주
- ⑤ 개인정보 보유 기간
- ⑥ 개인정보 보호를 위한 기술적 관리적 보호조치
- ⑦ 개인정보가 EU 역외로 이전되는지 여부

### STEP 6

#### 외부 업체의 GDPR 준수 여부를 모니터링하고 있습니까?



만약 아웃소싱 등 외부 업체를 통하여 개인정보를 처리한다면 GDPR 준수를 입증할 수 있는 업체를 선정

하여야 합니다. 외부 업체와 계약을 체결하기 이전에 GDPR 준수 여부를 확인하고, 이에 대해 계약서에 명시할 수 있습니다.

## STEP 7

### 기업의 책임성 강화를 위한 다음 조항들을 검토하고 있습니까?



- ① 보다 안전한 개인정보보호를 위하여 DPO를 지정하고 있습니까?  
다만, 기업의 핵심 활동에 개인정보 처리가 포함되지 않는 경우, 개인정보 처리가 위험을 초래할 가능성이 낮은 경우, 대규모 처리가 아닌 경우 등에 DPO 지정은 의무가 아닙니다.
- ② 개인정보 처리에 대하여 영향평가의 필요 여부를 확인하고 있습니까?  
공공장소에서의 대규모 개인정보 모니터링과 같이 개인정보 처리가 위험을 초래할 가능성이 있는 경우 영향평가를 받을 필요가 있습니다.

위 체크리스트는 EU 집행위원회에서 GDPR의 이해를 돕기 위해 참고자료로 제작되었습니다. 내용에 포함되어 있는 체크리스트는 GDPR 전체의 내용을 포괄하지 않을 수 있으므로 해당 자료에만 의존한 의사결정에 대해 권장하지 않습니다.  
또한 본 제작물을 바탕으로 한 의사결정의 책임은 한국인터넷진흥원에 있지 않음을 알려드립니다.

• 찾아보기 •

**B**

**BCRs** 143, 144, 147, 150, 151, 152, 153,  
192, 195, 196

**D**

**Directive** 10, 12, 14, 19, 21, 24, 34, 35, 36,  
37, 49, 64, 80, 112, 149, 150, 170, 171, 172  
**DPO** 11, 15, 16, 19, 20, 28, 34, 81, 112, 114,  
120, 121, 122, 123, 124, 125, 126, 127, 132,  
133, 134, 135, 159, 161, 178, 191, 195, 199

**E**

**EDPB** 11, 130, 143, 144  
**EU 집행위원회** 11, 21, 63, 130, 149, 151, 176,  
189, 192, 196, 197, 199

**G**

**가명처리** 13, 20, 23, 29, 30, 38, 115  
**감독기구** 11, 14, 15, 17, 24, 25, 26, 28, 36,  
37, 40, 82, 83, 85, 88, 96, 119, 120, 121,  
122, 127, 128, 129, 130, 131, 132, 133, 135,  
143, 144, 145, 147, 148, 150, 151, 152, 157,  
159, 160, 161, 162, 164, 165, 166, 170, 171,  
174, 175, 177, 179, 180, 181, 184, 191, 192,  
193, 198  
**개인정보** 11, 12, 13, 14, 15, 16, 17, 20, 21,  
22, 23, 24, 25, 26, 27, 28, 29, 30, 34, 36,  
37, 38, 39, 40, 41, 44, 45, 46, 47, 49, 50, 51,  
52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 63, 64,  
65, 70, 71, 72, 73, 74, 75, 76, 77, 80, 81, 82,  
84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95,  
96, 97, 98, 99, 100, 105, 106, 107, 108, 112,  
113, 114, 115, 116, 117, 118, 119, 120, 121,

122, 123, 124, 125, 126, 127, 129, 130, 132,  
133, 134, 135, 136, 137, 138, 139, 142, 143,  
144, 145, 146, 147, 148, 149, 150, 151, 152,  
156, 157, 158, 159, 160, 161, 162, 163, 164,  
165, 170, 172, 175, 177, 178, 179, 180, 181,  
189, 190, 191, 192, 193, 194, 195, 196, 197,  
198, 199

**개인정보보호** 10, 11, 16, 18, 19, 23, 25, 27,  
28, 29, 34, 35, 46, 53, 54, 57, 58, 65, 66, 75,  
76, 77, 112, 115, 116, 117, 125, 126, 128,  
130, 131, 132, 133, 134, 143, 145, 146, 148,  
149, 150, 151, 152, 192, 195, 196, 199

**개인정보 이동권** 11, 15, 34, 80, 95, 96, 97, 191

**개인정보 이전** 37, 52, 96, 142, 143, 144, 146,  
149, 152, 181, 196

**개인정보 처리** 12, 13, 14, 15, 17, 21, 22, 23,  
24, 25, 26, 27, 28, 29, 30, 38, 39, 40, 41, 44,  
45, 46, 47, 49, 50, 51, 52, 53, 56, 57, 58, 59,  
64, 70, 71, 72, 73, 75, 76, 77, 81, 84, 85, 87,  
89, 92, 93, 94, 98, 99, 107, 108, 112, 113,  
114, 115, 116, 117, 119, 121, 122, 123, 124,  
125, 126, 129, 132, 133, 134, 135, 136, 137,  
139, 149, 170, 170, 172, 175, 177, 178, 179,  
181, 189, 190, 191, 194, 195, 196, 197, 198,  
199

**개인정보 처리의 최소화** 13, 45, 107, 115

**개인정보 침해** 11, 15, 16, 17, 25, 112, 129,  
156, 157, 158, 159, 160, 161, 162, 163, 164,  
165

**개인정보 침해 통지** 11, 15, 16, 25, 129, 159,  
162, 163

**공동 컨트롤러** 70, 71, 77, 114, 173, 190

**공익을 위한 기록 보존** 30, 44, 62, 91

과징금 11, 17, 162, 165, 174, 175, 177, 178,  
179, 180, 181, 192  
과학적·역사적 연구 목적 44, 62  
관련 감독기구 131, 160  
구속력 있는 기업 규칙 16, 143, 144, 145, 148,  
151, 192, 195, 196  
구제 16, 83, 88, 96, 144, 152, 160, 170, 171  
국제기구 15, 37, 114, 129, 142, 143, 144, 145,  
146, 175, 181  
기술적·관리적 조치 23, 30, 45, 46, 70, 74, 76,  
105, 115, 127, 130, 165, 178, 179,  
기업 10, 11, 16, 23, 34, 35, 36, 47, 80, 104,  
112, 113, 114, 115, 125, 126, 127, 128, 130,  
132, 142, 143, 144, 145, 148, 150, 152, 153,  
180, 189, 190, 191, 192, 193, 195, 196, 199

## C

대리인 72, 73, 81, 114, 121  
대리인 지정 72  
동의 11, 13, 14, 16, 35, 38, 47, 49, 50, 51,  
52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63,  
82, 90, 93, 95, 104, 107, 129, 149, 175, 181,  
190, 191, 192, 194, 197  
동의 조건 49, 52, 53  
동의 철회 50, 51, 52

## D

명시적 동의 16, 38, 49, 54, 55, 56, 61, 104,  
146, 192, 194  
민감정보 12, 16, 20, 23, 27, 38, 55, 56, 61,  
63, 72, 104, 113, 118, 123, 137, 149, 179,  
191, 194, 195, 196  
반대권 15, 34, 80, 92, 98, 99, 100, 108

## B

범죄경력 및 범죄행위 16, 27, 63, 113, 118, 123,

179  
비례성 118

## 사

사법 구제 170, 171  
사전협의 28, 119, 120, 121, 122  
삭제권 15, 34, 80, 90, 91, 92, 108, 190  
생체 정보 27, 38, 61  
손해배상 172, 173, 181  
수령인 22, 82, 85, 93, 142, 143, 145, 146,  
149, 150, 175, 181, 198  
식별 가능 20, 21, 23, 29, 180, 189, 193  
선임 감독기구 11, 14, 24, 26, 164

## 아

아동 개인정보 13, 57, 60  
아동의 동의 57, 58, 60  
암호화 17, 96, 157, 158, 162, 165  
역사적 연구 목적 44, 62  
역외 이전 11, 15, 16, 25, 55, 56, 130, 133,  
142, 152, 192, 194, 195  
열람권 15, 20, 80, 85, 87, 108, 151, 175, 181  
영향평가 11, 15, 25, 106, 112, 117, 118, 119,  
120, 121, 122, 126, 135, 136, 138, 191, 192,  
195, 199  
유럽 개인정보보호 이사회 11, 130, 144  
유전정보 12, 21, 62  
유효한 동의 49, 50, 55, 56, 146  
익명처리 21, 29, 107, 164  
익명처리된 정보 21, 164  
인증 16, 17, 18, 96, 112, 128, 130, 131, 145,  
148, 151, 152, 179, 180, 193  
인증기관 17, 130, 131, 145, 175, 181  
인증기관에 대한 인가 11, 130, 131  
입증 책임 99  
잊힐 권리 80, 90, 91, 190

**ㄱ**

**자동화** 11, 15, 23, 39, 41, 52, 55, 56, 66, 80, 82, 86, 95, 100, 101, 102, 103, 104, 105, 106, 107, 108, 118, 136, 137, 191, 195

**자동화된 의사결정** 11, 15, 55, 56, 80, 101, 102, 104, 105, 107, 136, 137

**자동화된 처리** 101, 102, 118

**적절한 보호조치** 16, 52, 62, 105, 107, 114, 143, 144, 145, 146, 148

**적정성 결정** 16, 52, 143, 144, 145, 146, 148

**적정성 평가** 143, 144

**전자적 수단** 24, 53, 55, 83

**정당한 이익** 14, 81, 98, 99, 118, 129, 146, 148

**정보사회서비스** 13, 24, 57, 58, 60, 90, 190

**정보 제공** 66, 83, 107, 126

**정정권** 15, 35, 80, 88, 89, 90

**중대한 이익** 14, 47, 62, 146

**ㄴ**

**책임성** 11, 13, 15, 34, 46, 80, 106, 112, 128, 160, 194, 199

**처리 수단** 41, 115

**처리의 적법성** 13, 47, 48, 170

**처리 제한** 63, 85, 89, 91, 92, 94

**처리 제한권** 15, 34, 80, 92, 108

**추가적 정보** 23, 29, 30

**ㄷ**

**컨트롤러** 14, 15, 17, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 37, 39, 46, 47, 48, 50, 51, 52, 53, 54, 55, 56, 58, 59, 61, 64, 65, 66, 70, 71, 72, 73, 74, 75, 76, 77, 81, 82, 83, 84, 85, 86, 88, 90, 91, 92, 93, 95, 96, 98, 99, 100, 103, 104, 105, 106, 112, 114, 115, 117, 118, 120, 121, 122, 123, 124, 125, 126, 127, 129, 130, 131, 132, 138, 143, 144, 145, 146, 147,

148, 149, 150, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 171, 172, 173, 175, 176, 178, 179, 180, 181, 190, 191, 193, 194, 195, 196

**ㄹ**

**통계 목적** 30, 44, 62, 91, 98, 100, 124

**통지** 11, 14, 15, 16, 25, 55, 59, 60, 64, 66, 75, 83, 84, 87, 89, 94, 97, 100, 129, 145, 148, 150, 159, 160, 161, 162, 163, 164, 165, 166, 170, 180

**통지 의무** 157, 159, 160, 161, 162, 164, 166

**투명성** 11, 13, 18, 44, 51, 64, 80, 105, 107, 119, 128, 130

**ㅍ**

**파일링 시스템** 39, 41, 93

**표준 개인정보보호 조항** 16, 19, 25, 143

**프로세서** 14, 15, 16, 17, 19, 22, 24, 25, 26, 27, 28, 29, 37, 39, 61, 72, 73, 74, 76, 77, 114, 115, 120, 123, 126, 127, 129, 130, 132, 133, 134, 142, 143, 144, 145, 149, 150, 157, 160, 162, 172, 173, 175, 176, 178, 180, 181, 190, 191, 192, 193, 194, 195

**프로파일링** 11, 15, 23, 55, 56, 80, 82, 86, 98, 101, 102, 103, 104, 105, 106, 107, 108, 194

**ㅎ**

**행동규약** 16, 70, 112, 120, 121, 128, 129, 131, 143, 145, 148, 151, 175, 179, 180, 181

**협력** 37, 135, 161

## 집필진·자문·감수

연구책임기관	행정안전부 개인정보보호협력과 방송통신위원회 개인정보보호협력팀 한국인터넷진흥원 개인정보협력팀
외부 집필진 (가나다 순)	김경하 제이앤씨큐리티 대표 김도엽 고려대학교 정보보호대학원 변호사 성경원 SK인포섹 이사 윤수영 이베이코리아 팀장 이진규 네이버 이사 정윤정 법무법인 김·장 위원 조수영 숙명여자대학교 교수
외부 자문	이창범 동국대학교 겸임교수/산업보안센터장 서동태 LGCNS 책임 이성환 LGCNS 책임
법률 감수	김도엽 고려대학교 정보보호대학원 변호사 박광배 법무법인 광장 변호사

## 우리 기업을 위한 'EU 일반 개인정보보호법(GDPR)' 가이드북

발행일 2018년 5월

발행처 한국인터넷진흥원  
(58324) 전라남도 나주시 진흥길 9  
Tel. 1544-5118

디자인·제작 호정씨애플 Tel. (02) 2277-4718

문의 E-mail : [gdpr@kisa.or.kr](mailto:gdpr@kisa.or.kr), 전화 : 061-820-1805

1. 이 가이드북은 행정안전부와 방송통신위원회의 출연사업금으로 수행한 개인정보 보호 국제협력, 개인정보보호 국제협력 강화 사업의 결과입니다.
2. 이 가이드북의 내용을 발표할 때에는 반드시 한국인터넷진흥원 개인정보보호 국제협력, 개인정보보호 국제협력 강화 사업 결과임을 밝혀야 합니다.
3. 이 가이드북의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.