

우리기업을 위한
2022
EU일반개인정보
보호법가이드북

European Union General Data
Protection Regulation





머리말

개인정보를 처리하는 우리나라 사업자가 시의적절하게 활용하여
글로벌 시장에서 경쟁력을 확보할 수 있도록
『2022 EU 일반 개인정보보호법(GDPR) 가이드북』을
발간하였습니다.



우리나라에서 GDPR 가이드북을 발간하게 된 배경

2016년 5월 유럽연합(이하 'EU')에서 제정한 「일반 개인정보보호법(General Data Protection Regulation)」(이하 'GDPR')이 2018년 5월 25일부터 시행되었습니다.

GDPR은 기존의 EU 개인정보보호 지침인 「1995년 개인정보보호 지침(Data Protection Directive 95/46/EC)」을 대체하며 보다 강력한 제재를 규정하고 있습니다.

이에 한국인터넷진흥원은 「우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 안내서」(2017.04.)와 「우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 1차 가이드라인」(2017.11.)을 우선 발간하여 GDPR 시행 이전에 기업들의 사전 조치 수준을 제고하는 데 도움을 드리고자 하였습니다. 이후 GDPR 본격 시행에 따라 위 「안내서」와 「1차 가이드라인」의 내용을 통합하고, EU의 정책자문 기구 'The Article 29 Data Protection Working Party'¹(이하 '제29조 작업반')에서 발표한 보고서 내용을 포함해 「우리 기업을 위한 EU 일반 개인정보보호법(GDPR) 가이드북」(개정판, 2018.08)을 발간하였습니다.²

GDPR의 본격 시행 이후 GDPR 위반에 따른 과징금 부과사례들이 증가하고 있는 가운데, 영국, 프랑스, 일본 등 주요 국가들은 기업들의 GDPR 준수를 지원하기 위해 GDPR 해설 혹은 가이드를 제공하고 있습니다. 이에 한국인터넷진흥원은 우리 기업들에게 GDPR 준수에 대한 실질적이고 구체적인 가이드를 제공하기 위하여 주요 국가의 가이드 및 최근 EU 판결이나 과징금 부과사례 등을 참조하여 「2020 EU 일반 개인정보보호법(GDPR) 가이드북」(2020.07)을 발간하였습니다.

이번에 발간하는 「2022 EU 일반 개인정보보호법(GDPR) 가이드북」은 '2020년 가이드북'의 개정·증보판입니다. 주요 개정·증보 내용은 ▲EU의 우리나라에 대한 적정성 결정(Adequacy Decision) ▲EU에서 제3국으로 개인정보를 이전할 때 수출자와 수입자 사이에 체결해야 하는 표준계약조항(Standard Contractual Clauses, SCC) 개정 ▲브렉시트 이후 영국의 개인정보 정책 관련 변경·신규 사항 등입니다. 특히 EU의 우리나라 적정성 결정으로 우리 기업들은 EU시민의 개인정보를 추가 인증이나 절차 없이 국내로 이전할 수 있게 되었습니다. 모쪼록 '2022년 가이드북'이 우리 기업의 GDPR 준수에 실질적인 도움이 되기를 바랍니다.

¹ 제29조 작업반(The Article 29 Working Party, WP29): Directive에 의거해 설립된 '개인정보보호 작업반(Data Protection Working Party)'의 약칭으로, EU 역내 각 회원국의 감독기구 대표들로 구성된 개인정보보호 정책 자문 기관이다. GDPR 시행과 함께 유럽 개인정보보호 이사회(European Data Protection Board, EDPB)로 대체되었다(전문 제139항).

² 이 가이드북 공개 이후 민·관의 의견에 따라 문장 일부를 개선하여 개정판(2018.08)으로 재공게 되었다.

국가명	발행기관	가이드제목	발행일
일본	JETRO	EU GDPR 가이드(입문편)	2016. 11.
		EU GDPR 가이드(실천편)	2017. 08.
프랑스	CNIL	프로세서를 위한 GDPR 가이드	2017. 09.
영국	ICO	GDPR 가이드	2019. 05. 22.
		Guidelines 3/2019	2019. 07. 10.
		Recommendation 01/2019	2019. 07. 10.
	EDPB	Guidelines 2/2019	2019. 04. 09.
		Guidelines 2/2019 Version 2.0	2019. 10. 08.
		Guidelines 1/2019 Version 2.0	2019. 06. 04.
		Guidelines 4/2018 Version 3.0	2019. 06. 04.
		Guidelines 3/2018 Version for public consultation	2018. 11. 16.
		Guidelines 2/2018	2018. 05. 25.
		Guidelines 1/2018 Version 3.0	2019. 06. 04.
		Endorsement 1/2018	2018. 01.
	ARTICLE 29 DATA PROTECTION WORKING PARTY	동의 가이드라인	2018. 04. 10.
		투명성 가이드라인	2018. 04. 11.
		자동화된 개인별 의사결정과 프로파일링 가이드라인	2018. 02. 06.
		개인정보침해 고지 가이드라인	2018. 02. 06.
		개인정보 이동권 가이드라인	2017. 04. 05.
		개인정보 영향평가 가이드라인	2017. 10. 04.
		DPO 가이드라인	2017. 04. 05.
		주 감독기구 확인을 위한 가이드라인	2017. 04. 05.
		기록 유지 의무 면제에 관한 입장문	2018. 04. 19.

※ 해외의 GDPR 가이드에 대한 자세한 현황은 [참고자료] 5. 해외의 GDPR 가이드 현황 참조



가이드북을 발간하게 된 목적

이 가이드북은 GDPR이 규정하는 개인정보의 처리와 관련한 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 작성되었습니다.

또한 우리 기업이 GDPR의 전반적인 이해를 통하여 기업 생태계에 맞는 개인정보보호 기반을 구축하고 EU를 비롯한 글로벌 시장에서 경쟁력을 제고하는 데 그 목적이 있습니다.



2022년 가이드북 주요 수정·보완 내용

“우리 기업을 위한 2022 EU 일반개인정보보호법 가이드북”은 2년 전 발간한 “2020 가이드북”의 수정·증보판으로서 지난 2년 간 있었던 주요 사건과 개정된 사항들을 담았습니다. “2022 가이드북”에 수정하고 새로 수록한 주요 내용은 다음과 같습니다.

- (EU와 우리나라의 적정성 결정) EU와 우리나라는 상호 개인정보보호법의 규율 내용과 수준이 동등하다고 판단하고 2021년 12월 17일 ‘개인정보보호 적정성 결정(Adequacy Decision)’을 내렸습니다. 이에 따라 우리나라 기업들은 EU 시민의 개인정보를 별도의 까다로운 절차나 인증 없이 국내로 이전할 수 있게 되었습니다. (관련 페이지: 213~214)
- (EU 표준계약조항 개정) EU는 적절한 보호조치를 통한 개인정보 역외 이전 방법으로 구속력 있는 기업 규칙(BCR, Binding Corporate Rules), 표준 개인정보보호 조항(Standard Data Protection Clauses) 또는 표준계약조항(SCC, Standard Contractual Clauses) 등의 제도를 두고 있는데, 이중 표준 개인정보보호 조항을 2021년 6월에 개정해 시행하고 있습니다. 개정사항으로 EU 역내에서 역외로 이전하는 유형을 4가지로 구분하였는데 해당 내용을 담았습니다. (관련 페이지: 215~216페이지)

우리기업을 위한

2022

EU일반개인정보 보호법가이드북

European Union General Data
Protection Regulation

● (영국의 EU 탈퇴와 개인정보보호) 영국은 2020년 1월 31일부로 정식으로 EU를 탈퇴하였습니다. 이에 따라 영국은 더 이상 EU GDPR에 의거해 개인정보보호를 규율하지 않고, 자국의 ▲UK GDPR ▲개인정보보호법 2018(Data Protection Act 2018, DPA 2018) ▲프라이버시 전자통신 규정(Privacy and Electronic Communications Regulation 2003, PECR) 등을 통해 개인정보보호 준수를 요구합니다. 이밖에 영국 정부는 최근 (2022년 11월 23일) 우리나라에 대해 적정성 결정에 관한 입법 절차를 완료하였다고 발표하였습니다. 이후 영국의 우리나라에 대한 적정성 결정이 올해 안에 의회를 통과할 예정입니다. 적정성 결정이 최종 통과되면 영국 내 우리 기업들의 영국 국민 개인정보 이전이 별도의 절차나 인증 없이 가능해 질 것입니다. (관련 페이지: 280~281)

● (기타) 이밖에 ▲GDPR 위반에 대한 주요 과징금 부과사례 (249~251페이지) ▲GDPR 적용 대상 국가의 감독기구 현황(261~265페이지) ▲해외 GDPR 관련 가이드 발간 현황 (282~290페이지) 등에서 변경된 내용을 수정하고 새로운 내용을 추가하였습니다.

01

개요

1. GDPR의 제정 의미와 효력

1.1 GDPR 제정 목적과 의의	18
1.2 GDPR의 구성	19
1.3 GDPR의 법적 효력	19

2. GDPR 시행에 따라 유의해야 할 주요 사항

2.1 EU 역내 및 역외 적용	21
2.2 개인정보 정의와 적용대상 범위	21
2.3 개인정보 기본 처리 원칙	22
2.4 동의 요건의 강화 및 아동 개인정보 처리에 대한 동의 원칙	22
2.5 개인정보의 합법처리 기준	22
2.6 one stop shop 메커니즘의 도입	23
2.7 프로세서에 대한 적용	23
2.8 정보주체의 권리	24
2.9 책임성과 거버넌스	24
2.10 DPO 지정 의무	24
2.11 개인정보 역외 이전 메커니즘	25
2.12 개인정보 침해 시 통지의무	25
2.13 제재	26
2.14 인증제도 및 인증기관에 대한 인정	26

3. GDPR 내 주요 용어

3.1 주요 용어의 표기	27
3.2 주요 용어의 정의	28

4. GDPR의 적용 대상과 범위

4.1 적용 대상(제1조)	38
4.2 적용 범위	41
4.3 적용 예외(National derogations)(제2조제2항)	43

02

개인정보 처리기준

1. 개인정보 처리 원칙

1.1 합법성·공정성·투명성의 원칙	47
1.2 목적 제한의 원칙	49



1.3 개인정보 최소화처리 원칙	53
1.4 정확성 원칙	57
1.5 보유기간 제한의 원칙	63
1.6 무결성·기밀성의 원칙	69
1.7 책임성의 원칙	71
2. 처리의 합법성	
2.1 합법처리의 근거	75
2.2 동의	81
2.3 계약	83
2.4 법적 의무 준수	90
2.5 중대한 이익	93
2.6 공적 업무 수행	95
2.7 적법한 이익 추구	98
3. 동의	
3.1 동의의 정의	104
3.2 동의의 유효 요건	104
3.3 명시적 동의가 필요한 경우	109
3.4 동의의 철회	110
4. 아동 개인정보	
4.1 개요	112
4.2 아동에게 제공되는 온라인 서비스	113
4.3 친권자 동의	113
4.4 친권자의 동의를 확인하는 방법	115
4.5 아동에 대한 통지	116
5. 민감정보 및 범죄정보	
5.1 민감정보의 처리 제한	117
5.2 범죄정보의 처리 금지	119

03

정보주체의 권리 보장

1. 개요	124
2. 정보를 제공받을 권리(Right to be informed)	
2.1 주요 내용	125
2.2 개인정보의 수집 시 정보 제공 의무	126
2.3 정보주체의 요청 시 정보제공 의무	129
2.4 정보 제공 방법	130
2.5 추가 처리	133
2.6 적용 제외	134
2.7 최근 과징금 사례	134
3. 정보주체의 접근권(Right of access by the data subject)	
3.1 주요 내용	136
3.2. 국외 이전 시	137
3.3 접근 요구 시 조치 사항	137
4. 정정권(Right to rectification)	
4.1 주요 내용	139
4.2 정정 요구 시 조치 사항	140
4.3 정정 요구를 거절할 수 있는 사유	140
5. 삭제권(‘잊힐 권리’)[Right to erasure(‘Right to be forgotten’)]	
5.1 주요 내용	142
5.2 개인정보가 공개된 경우	144
5.3 삭제 거부 가능한 경우	144
5.4 최근 사례	144
6. 처리 제한권(Right to restriction of processing)	
6.1 주요 내용	146
6.2 처리가 가능한 경우	147
6.3 처리 제한 해제 시	147
7. 개인정보 이동권(Right to data portability)	
7.1 주요 내용	149
7.2 이동권 요구 시 조치 사항	151



8. 반대권(Right to object)

8.1 주요 내용	153
8.2 반대권 요구 시 조치 사항	154
8.3 온라인 서비스의 경우: 자동화된 방식으로 이의 제기가 가능해야 함	155

9. 프로파일링을 포함한 자동화된 의사결정

(Automated individual decision-making, including profiling)

9.1 프로파일링 및 자동화된 의사결정의 개념	156
9.2 정보 주체의 권리	158
9.3 적용 예외	159
9.4 자동화된 의사결정 수행 시 조치 사항	160

04

기업의 책임성
강화

1. 개요

168

2. 개인정보 처리 활동의 기록

2.1 처리 활동 기록이 필요한 경우	170
2.2 처리 활동 기록 대상	170

3. Data protection by design and by default

3.1 'Data protection by design and by default'의 의미	172
--	-----

4. 개인정보 영향평가

4.1 개요	175
4.2 개인정보 영향평가 대상	176
4.3 개인정보 영향평가 수행 절차	178
4.4 개인정보 영향평가 관련 내·외부 협의 체계	179

5. DPO(Data Protection Officer) 지정

5.1 DPO 지정	185
5.2 DPO의 자질	188
5.3 DPO의 업무	189
5.4 DPO의 지위	190
5.5 고용주(Employer)의 의무	191
5.6 DPO의 책임 여부	191

6. 행동규약과 인증

6.1 행동규약과 인증제도 권장	192
6.2 행동규약의 작성	194
6.3 행동규약 준수에 대한 모니터링	195
6.4 인증제도(제42조)	195
6.5 인증기관	197

05

개인정보의 역외 이전

1. 개인정보 역외 이전에 관한 총칙(제5장)	208
2. EU 역외로 개인정보 이전이 가능한 경우(제45조~제47조)	
2.1 적정성 결정에 따른 이전(Transfer on the basis of an adequacy decision)	213
2.2 우리나라의 EU 적정성 결정(adequacy decision) 획득	214
2.3 적절한 보호조치(Appropriate safeguards)에 의한 이전	215
3. EU 역외로 개인정보 이전이 가능한 예외적인 특정 상황(제48조 및 제49조)	

06

개인정보 침해 발생 시 조치 사항

1. 개인정보 침해	
1.1 개인정보 침해의 개념	229
1.2 개인정보 침해 사고의 인지	231
2. 개인정보 침해 통지	
2.1 감독기관에 대한 통지 의무	233
2.2 정보주체에 대한 통지 의무	235
2.3 위반 시 과징금	237

07

피해 구제 및 제재

1. 구제수단	
1.1 감독기관에 민원을 제기할 권리	245
1.2 감독기관의 결정에 관한 사법적 구제 수단	245
1.3 컨트롤러 또는 프로세서에 대한 효과적인 사법적 구제 수단에 관한 권리	246
2. 손해배상청구권 및 책임	
2.1 컨트롤러와 프로세서의 손해배상 의무	247
2.2 프로세서의 손해배상 의무	248
2.3 책임 면제	248



3. 과징금	
3.1 원칙	249
3.2 최대 과징금	249
4. 벌칙	252
참고자료	259

표 목 차

표 1	GDPR의 구성 체계	19
표 2	개인정보와 개인정보가 아닌 정보	29
표 3	EU 회원국의 친권자 동의가 필요한 아동 연령	113
표 4	정보주체의 권리 강화에 대한 내용 및 관련 주요 조문	124
표 5	기업의 책임성 강화와 관련한 내용 및 조문	168
표 6	개인정보 처리 활동의 기록 내용	171
표 7	ICO 개인정보 영향평가 양식 예시	183
표 8	EU 적정성 결정 절차	214
표 9	표준계약조항(SCC)에서 구분하는 4가지 모듈과 상황	217
표 10	개인정보 침해에 대한 감독기구 통지 필요 여부 판단 예시	240
표 11	개인정보 침해에 대한 정보주체 통지 불필요 예시	241
표 12	주요 과징금 부과 사례	250

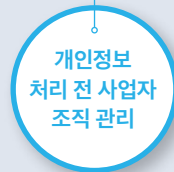
그림목차

그림 1	EU의 법체계	20
그림 2	ICO 개인정보 영향평가 절차	182
그림 3	DPO 지정 의사결정 절차	187
그림 4	DPO 지정 시 고려사항	198
그림 5	개인정보 처리 시 높은 위험의 판단 기준	202
그림 6	개인정보 역외 이전 메커니즘	209
그림 7	개인정보 역외 이전 흐름도	210
그림 8	개인정보 침해 통지 흐름도	238

개인정보 Lifecycle과 GDPR 주요 규정

Lifecycle & GDPR

- 개인정보보호중심설계(DPD)(§25)
- DPO(§37~§39)
- 처리활동 기록(§30)
- 처리의 안전성 확보(§32)
- 개인정보영향평가(§35)
- 행동규약(§40~§41)
- 인증(§42)



- 감독기구와의 협력(§31)
- 사전 자문(§36)
- 과징금(§83)
- 제재(§84)

사업자는 개인정보 처리에 따른 위험 수준을 자체적으로 판단하여
개인정보의 관리 단계별 GDPR 상 주요 의무를 준수하여야 한다.

- 적용범위(§2, §3)
- 처리원칙(§5)
- 합법처리기준(§6)
- 동의요건(§7, §8)
- 민감정보(§9)
- 범죄정보(§10)
- 공익, 과학적·역사적 연구, 통계
목적 처리 시 안전조치(§89)

- 역외이전 일반원칙(§44)
- 적정성 결정에 의한 이전(§45)
- 적절한 안전조치에 따른 이전(§46)
- 구속력 있는 기업규칙에 의한 이전(§47)
- 특정 상황 하에서의 예외(§49)

개인정보
수집 등 처리

개인정보
역외이전

- 입법목적(§1)
- 물적 적용범위(§2)
- 장소적 적용범위,
역외적용(§3)
- 용어 정의(§4)

개인정보
유출 등 침해시

정보주체
권리 행사 시

- 감독기관에 대한 통지(§33)
- 정보주체에 대한 통지(§34)

- 접근권(§15)
- 정정권(§16)
- 삭제권(잊힐 권리)(§17)
- 처리제한권(§18)
- 고지의무(§19)
- 개인정보 이동권(§20)
- 거부권(§21)

- 프로파일링 등 자동화된
의사결정(§22)
- 민원을 제기할 권리(§77)
- 효과적인 사법구제
받을 권리(§78, §79)
- 보상 및 책임(§82)



01

개요



1. GDPR의 제정 의미와 효력
2. GDPR 시행에 따라 유의해야 할 주요 사항
3. GDPR 내 주요 용어
4. 적용 대상과 범위



GDPR의 제정 의미와 효력



Point

- GDPR 시행의 의미를 알 수 있다.
- GDPR의 전체적인 구성을 알 수 있다.
- GDPR의 법적인 효력을 알 수 있다.

1.1 GDPR 제정 목적과 의의

- GDPR은 자연인(natural person)에 관한 기본권과 자유(특히 개인정보보호에 대한 권리)를 보호하고(제1조제2항), EU 역내에서 개인정보의 자유로운 이동(제1조제3항)을 보장하는 것을 목적으로 한다.
- GDPR은 개인정보 삭제권, 처리 제한권, 개인정보 이동권, 반대권(거부권) 등의 신규 권리 추가 및 기존 권리 명확화를 통하여 기존 Directive 95/46/EC보다 정보주체의 권리를 확대·강화하였으며, 개인정보 처리 활동의 기록, DPO의 지정, 개인정보 영향평가, Data protection by design and by default 등을 규정함으로써 기업의 책임성을 강화하였다.

GDPR 관련 규정	■ 제1조(대상 및 목적)
한국 개인정보보호법 관련 규정	■ 제1조(목적)

1.2 GDPR의 구성

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

※ GDPR 원문은 EU 공식 홈페이지³를 통해 내려받을 수 있다.

| 표 1. 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 구제, 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)	

1.3 GDPR의 법적 효력

- GDPR은 지침(Directive)과 달리 “Regulation”이라는 법 형식으로 제정되어 법적 구속력을 가지며, 모든 EU 회원국 내에 직접적으로 적용된다(제99조).

기존 Directive에서는 회원국 간 개인정보보호 법제가 서로 달라 규제에 어려움이 있었으나, GDPR 제정을 통하여 통일된 개인정보보호 규제가 가능하게 되었다.

※ Directive는 각 회원국에 대한 입법 지침(가이드라인) 역할을 할 뿐이므로, 회원국 내 적용을 위해서는 지침을 반영한 각국의 개별 입법이 필요하다.

3 Publications Office of the European Union, Regulation(EU) 2016/679 of the European Parliament and of the Council, 2016. 04. 27. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ.L.:2016:119:TOC

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

※ 그동안 시행되어 온 Directive 95/46/EC는 2018년 5월 25일 GDPR 시행으로 폐지되었다(전문 제171항).

| 그림 1. EU의 법체계





GDPR 시행에 따라 유의해야 할 주요 사항



Point

- GDPR의 주요 준수 사항을 확인한다.
- 개인정보의 생명주기(lifecycle)에 따라 준수하여야 할 GDPR 규정을 확인한다.

2.1 EU 역내 및 역외 적용

- 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 경우

※ 유럽 경제 지역(European Economic Area, EEA)에 관한 주요 협정 제7조(a)에 따라
아이슬란드, 리히텐슈타인, 노르웨이도 EU와 동일하게 GDPR이 적용

2.2 개인정보 정의와 적용대상 범위

- 개인정보를 “식별되었거나 또는 식별 가능한 자연인(정보주체)과 관련된 모든 정보”로 정의하면서(제4조제1항), 기존 Directive에 명시되지 않았으나 판례, 유권해석, 개별법 차원에서 인정된 개념을 포함하였다.

- ① 자연인이 사용하는 장치, 애플리케이션, 도구와 프로토콜을 통해 제공되는 개인 식별이 가능한 경우의 IP 주소, 쿠키(cookie) ID, RFID(무선 인식) 태그 등을 개인정보(온라인 식별자)에 포함한다(전문 제30항).
- ② 위치정보를 개인정보의 정의에 명시적으로 규정하였다(제4조제1항).
- ③ 민감한 성격의 개인정보를 ‘특수한 범주의 개인정보’(이하 ‘민감정보’)라고 정의하면서, 유전정보와 생체 인식정보를 명시적으로 규정하였다(제9조제1항).

- ④ 개인정보의 가명처리(pseudonymisation) 개념을 명문화함으로써(제4조제5항),
 분리 보관 및 특별조치 등을 통하여 개인정보를 활용할 수 있도록 하였다.

2.3 개인정보 기본 처리 원칙

- 개인정보를 처리하는 경우 다음 7가지 원칙을 모두 준수하여야 한다(제5조).
- ① 합법성·공정성·투명성 원칙
 - ② 목적 제한의 원칙
 - ③ 개인정보 최소화처리 원칙
 - ④ 정확성의 원칙
 - ⑤ 보유기간 제한의 원칙
 - ⑥ 무결성과 기밀성의 원칙
 - ⑦ 책임성의 원칙

2.4 동의 요건의 강화 및 아동 개인정보 처리에 대한 동의 원칙

- GDPR에 따른 유효한 동의는 수집되는 개인정보가 이용되는 목적에 대한 명시적 동의여야 한다(GDPR 제7조 및 제4조). 컨트롤러는 동의를 받았다는 사실을 증명할 수 있어야 하고, 해당 동의는 철회될 수 있다.
- 만 16세 미만의 아동에게 직접 정보사회서비스를 제공할 때에는 부모나 보호자의 동의를 받아야 한다(제8조제1항). 다만, 각 회원국은 개별 법률을 통하여 부모나 보호자의 동의를 요하는 아동의 연령 기준을 만 13세까지 낮추어 규정할 수 있다(제8조제2항).

2.5 개인정보의 합법 처리 기준

- 개인정보 처리의 합법성: 공정성·투명성 원칙에 따라 개인정보 처리는 GDPR에서 허용한 다음 중 어느 하나 이상의 요건에 해당해야 합법 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 자연인인 제3자의 생명상의 이익을 보호하기 위하여 처리가 필요한 경우
- ⑤ 공익상의 이유 또는 컨트롤러에게 부여된 직무권한을 행사할 때 처리가 필요한 경우
- ⑥ 컨트롤러 또는 제3자의 적절한 이익을 달성하기 위하여 처리가 필요한 경우

2.6 One Stop Shop 메커니즘의 도입

- 원스톱숍 메커니즘(One stop shop mechanism)이란 처리되는 개인정보의 정보주체가 EU 내 여러 국가에 흩어져 있는 경우에 주 사업장이나 단일 사업장이 소속된 국가의 감독기구가 주 감독기구의 역할을 수행하면서 다른 회원국의 감독기구와 수시로 협력함으로써 컨트롤러·프로세서가 하나의 감독기구만을 대상으로 대응 가능한 집행 체계를 말한다.

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

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

2.7 프로세서에 대한 적용

- GDPR은 프로세서를 직접 규제하는 다음 내용을 다수 포함하고 있어서, 프로세서도 개인정보보호를 위한 다양한 의무를 부담한다.

- 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(제44조~제50조)]
- ⑤ 국가 감독기구 협조 의무(제31조) 등

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

2.8 정보주체의 권리

- ① 접근권(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

- 공공 기관이나 정기적·체계적·대규모 등 일정 기준에 해당하는 컨트롤러나 프로세서는 DPO(Data Protection Officer)를 지정해야 하고(제37조~제39조), 컨트롤러에게도 GDPR 각 규정의 준수를 위하여 일정한 의무가 부과된다. 예를 들면, 문서보관의무나 개인정보 영향평가(제35조)를 받을 의무가 있으며, 기획 단계에서부터 기본적으로 정보보호가 높은 수준으로 설정될 수 있도록 관련활동을 수행하여야 한다(privacy by design and by default, 제25조). 구체적으로 개인정보보호를 위하여 아래와 같은 책임성 및 거버넌스가 요구된다.
 - ① 처리 활동의 기록(제30조)
 - ② 높은 위험(high risk)을 내재한 개인정보 처리에 대하여 개인정보 영향평가 수행(제35조)
 - ③ DPO 지정(제37조)
 - ④ 개인정보 침해 통지 및 종합적 기록 유지(제33조~제34조)
 - ⑤ Data protection by design and by default 이행(제25조) 등

2.10 DPO 지정 의무

- 다음에 해당하는 경우 DPO를 의무적으로 지정해야 하며, DPO는 조직이 개인정보 보호 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

- GDPR이 인정하는 개인정보의 역외 이전 메커니즘에 따르는 경우에만 EU 역외로의 개인정보 이전이 허용된다.
 - ① 적정성 결정(adequacy decision)을 통하여 개인정보보호 관련 법제가 적절한 수준의 보호를 보장하고 있다고 인정된 국가로 이전하는 경우(제45조)
 - ② ‘적절한 보호조치(appropriate safeguards)의 제공’, ‘정보주체의 권리 행사 보장’, ‘효과적인 법적 구제 수단의 존재’에 모두 해당하는 경우(제46조)
 - 적절한 보호조치에는 구속력 있는 기업 규칙(Binding Corporate Rules), 표준 개인정보보호 조항(Standard data protection clauses), 승인된 행동규약(code of conduct), 승인된 인증 메커니즘(certification) 등이 포함
 - ③ 적정성 결정이나 적절한 보호조치가 없는 경우에도 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 시 통지의무

- 컨트롤러는 개인의 권리와 자유에 위협을 일으킬 가능성이 있는 침해가 발생한 경우, 개인정보 침해 사실을 인지한 시점으로부터 72시간 내에 감독기관에 신고하여야 하며, 개인의 자유와 권리에 높은 위험이 예상될 때에는 부당한 지체 없이(without undue delay) 침해 사실을 정보주체에게 통지하여야 한다.
- 다만 개인정보 침해가 개인의 자유와 권리에 위협을 일으킬 가능성이 낮은 경우 통지하지 않을 수 있다.
- 만약, 감독기관에 대한 신고가 72 시간 이내에 이루어지지 않는 경우에는 지체된 이유를 함께 신고해야 한다.

2.13 제재

- 각각의 개인정보 처리에 따라 제재 규정을 적용하며, ‘사업체 집단’ 매출을 바탕으로 과징금(fines imposed by reference to the revenues of an undertaking)을 부과한다.
 - ① GDPR 규정의 일반적 위반의 경우 직전 회계연도의 전 세계 매출액 2% 또는 1천만 유로 중 더 큰 금액을 상한으로 하여 부과
 - ② GDPR 규정의 심각한 위반의 경우 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 더 큰 금액을 상한으로 하여 부과

2.14 인증제도 및 인증기관에 대한 인정

- GDPR은 기업의 GDPR 준수 입증을 위해 인증 메커니즘(certification mechanism)의 이용을 권장하고 있다.

인증 제도를 활용할 경우 기업은 기술적·관리적 조치 및 개인정보 이전과 관련한 적절한 보호조치를 실시하고 있음을 입증할 수도 있다.
- 인증서는 감독기구나 지정된 인증기관이 발행하며 인증의 유효기간은 최대 3년이다.

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.



GDPR 내 주요 용어



Point

- GDPR에서 제시된 주요 용어의 개념을 이해할 수 있다.

3.1 주요 용어의 표기

- 이 가이드북은 앞서 발간된 ‘안내서’, ‘1차 가이드라인’ 및 ‘가이드북 개정판’에서 표기한 용어를 준용하는 것을 원칙으로 하나, GDPR에 명시된 내용에 따라 변경되어야 할 필요성이 있거나 부정확한 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 약자이다. 이는 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 ‘시스템 설계시 기본설정으로서의 개인정보보호’ 정도로 번역할 수도 있지만, 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), 접근권(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 access의 번역과 관련하여, 정보에 대한 공개는 정보주체의 자발적인 요청을 통한 열람을 내포하기 때문에 ‘열람권’이라는 용어를 사용하기도 하지만, 이 가이드북에서는 열람권이 해당 권리의 일부를 구성한다는 점과 원어의 의미를 가장 잘 나타내는 번역이 바람직하다는 점을 고려하여 ‘접근권’이라는 용어를 사용한다.

3.2 주요 용어의 정의

3.2.1 개인정보(Personal data)(제4조제1항)

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

개인과 관련되어 있는지의 여부를 판단할 때에는 정보의 내용(직·간접적으로 개인 또는 그들의 활동에 대한 것인지의 여부), 그 정보의 처리 목적, 그 정보를 처리함으로써 개인에게 미치는 영향이나 결과를 고려할 필요가 있다. 부정확한 정보라고 하더라도 식별 가능한 개인과 관련되어 있다면 개인정보일 수 있다.

■ 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.⁴ 개인을 직접 또는 간접적으로 식별 가능한 경우라면, 이름·전화번호 등과 같은 일반적인 개인정보 외에 온라인 식별자⁵나 위치정보도 GDPR이 정의하는 개인정보에 해당한다.

4 제29조 작업반, Opinion 4/2007 on the concept personal data, 2007. 04., pp.7~8.

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

개인정보의 구체적인 예로는 자연인의 성명, 식별번호, 소재지 정보, 메일주소, 온라인 식별자(IP주소, 쿠키 식별자), 신체적·생리학적·유전자적·정신적·경제적·문화적·사회적 고유성에 관한 요인 등이 있다.

표 2. 개인정보와 개인정보가 아닌 정보⁶

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

3.2.2 처리(제4조제2항)

- 개인정보의 ‘처리’란 자동적인 수단인지의 여부와 관계없이 개인정보 또는 개인정보의 집합에 대하여 행하는 단일의 작업 또는 일련의 작업을 말한다. 신용카드 정보의 보존, 메일 주소의 수집, 고객 연락처정보의 변경, 고객 성명의 공개, 상급자의 종업원 업무 평가 열람, 정보주체의 온라인 식별자 삭제, 전 직원의 성명이나 사내의 직무, 사업소의 주소, 사진을 포함한 명부의 작성 등이 모두 개인정보의 ‘처리’에 해당한다.

3.2.3 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. 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.

6 European Commission, "What is personal data?", 2020. 03. 16., https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

3.2.4 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.

3.2.5 수령인(Recipient)과 제3자(Third party)(제4조제9항~제10항)

- 수령인은 제3자인지 여부와 관계없이 개인정보를 공개·제공받는 자연인이나 법인, 정부 부처 및 관련기관, 기타 단체 등을 의미한다.

※ 예외적으로 EU 또는 회원국 법률에 따라 특정한 문의·회신 및 조화 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 알려주어야 하는 의무를 부담하므로, 수령인 또는 수령인의 유형을 사전에 식별할 필요가 있다.

제3자는 ① 정보주체, ② 컨트롤러, ③ 프로세서, ④ 컨트롤러·프로세서의 직접적 권한에 따라 개인정보를 처리할 수 있는 사람을 제외한 모든 자연인이나 법인, 정부부처 및 관공기관, 기타 단체 등을 의미한다.

3.2.6 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 개인정보(input personal data)와 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.

3.2.7 가명처리(Pseudonymisation)(제4조제5항)

- 추가적 정보의 사용 없이는 더 이상 특정 정보주체를 식별할 수 없도록 개인정보를 처리하는 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 가명처리 하는 경우, 해당 기업은 ① Data protection by design and by default 의무를 충족하는데 도움이 되고, ② 개인정보를 보호할 수 있는 보안적 수단으로써 장점 등을 가질 수 있다.

3.2.8 정보사회서비스(Information society service)(제4조제25항)

- 정보사회서비스란 서비스를 제공받는 자의 개별적 요청에 따라 원격으로 전자적 수단을 통하여 통상 영리 목적으로 제공되는 서비스를 의미한다.⁷
 - ※ 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 검색엔진을 의미한다.

⁷ Publications Office of the European Union, Directive(EU) 2015/1535 of the European Parliament and of the Council, 2015. 09. 09.

3.2.9 감독기구(supervisory authority)(제4조제21항~제22항)와 주 감독기구 (lead supervisory authority)

■ 감독기구

GDPR은 EU 회원국마다 하나 이상의 감독기구(supervisory authority 또는 data protection authority)의 설립을 의무화함으로써 컨트롤러와 프로세서의 개인정보 처리 활동에 대한 공조와 통제가 가능하도록 하고 있다. 감독기구는 다음 사유에 해당하는 경우 컨트롤러 또는 프로세서의 개인정보 처리에 관여할 수 있다.

- ① 컨트롤러나 프로세서가 자국 영토에 설립한 사업장에서 행하는 정보 처리
- ② 공익을 위하여 정부부처 및 관련기관이나 민간기구가 행하는 정보 처리
- ③ 자국 영토의 정보주체에 영향을 미치는 정보 처리
- ④ EU 역내에 설립되지 않은 컨트롤러나 프로세서가 해당 감독기구가 설립된 국가에 거주하는 정보주체를 대상으로 행하는 정보 처리 등(전문 제122항)

■ GDPR은 본문 전반에 걸쳐 다음과 같이 감독기구의 업무와 권한을 명시하고 있다(제 57조).

- 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 역의 이전에 대한 고지 접수
- ⑦ GDPR 시행과 관련한 조사 실시
- ⑧ 개인정보처리 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, 별도의 연간 공공 예산을 받아야 한다. 또한 다른 감독기구와의 상호 협력 및 지원과 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).

■ 주 감독기구⁸

다음에 해당하는 주 사업장 또는 단일 사업장을 관할하는 감독기구의 경우 주 감독기구(lead supervisory authority)가 된다.

- ① EU 내 하나 이상의 회원국에 배치된 컨트롤러나 프로세서의 주 사업장이 해당 감독기구가 소재한 국가에서 개인정보처리를 하는 경우
- ② EU 내 설립된 컨트롤러나 프로세서의 단일 사업장에서 시행되는 개인정보 처리가 하나 이상의 회원국의 정보주체에 실질적으로 영향을 미치거나(substantially affect) 미칠 가능성이 있는 경우(전문 제124항)

- 주 감독기구는 정보주체가 자신의 개인정보 처리에 대하여 민원을 제기할 때, 국경을 초월하는 개인정보 처리 활동을 다룰 1차적 책임이 있다. 이 때 주 감독기구는 관련있는 다른 감독기구의 모든 조사에 협력하게 된다.

GDPR 관련 규정	■ 제4조(정의)
한국 개인정보보호법 관련 규정	■ 제2조(정의)

⁸ 제29조 작업반, Guidelines on the lead supervisory authority, 2017. 04. 05., pp.4~5.

+ 더 알아보기 / 1

개인정보보호법과 GDPR의 주요 용어 비교

국내 개인정보보호법과 EU의 GDPR은 일부 유사한 용어를 사용하는 것처럼 보이나 그 범위 및 역할 등에서 상이한 용어가 존재한다. 따라서 아래의 주요 용어에 명시한 개념의 차이를 이해하고 GDPR 적용에 있어 혼란이 없도록 해야 한다.

한국(개인정보보호법)	EU(GDPR)	비고
특수한 범주의 개인정보(민감정보)	<p>[제9조] 컨트롤러는 인종·민족, 정치적 견해, 종교적·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체정보, 건강정보, 성생활·성적 취향에 관한 정보를 처리해서는 안 된다.</p> <p>[제10조] 범죄경력 및 범죄행위에 관련된 개인정보의 처리 또는 제6조제1항에 근거한 관련 보안조치는 공적권한의 통제 하에서 또는 그 처리가 정보주체의 권리 및 자유를 위한 적절한 안전장치를 규정하는 EU 또는 회원국 법이 허가하는 경우에만 수행되어야 한다.</p>	GDPR은 특수한 범주의 개인정보(민감정보)와 범죄 경력 및 범죄행위에 관련한 개인정보를 구분하고, 그 처리기준을 구분하였음
위탁자	컨트롤러	
<p>[제26조제2항] 위탁자는 개인정보의 처리 업무를 위탁하는 개인정보처리자를 의미한다.</p> <p>위탁자는 자신의 사무 처리를 위해 통상 직접수집한 개인정보를 수탁자에게 제공한다.</p>	<p>[제7조] 컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 주체를 의미한다.</p> <p>컨트롤러는 개인정보 처리의 목적과 수단을 규정하지만 하면 족하며, 자신이 개인정보를 직접 수집하여 프로세서에게 제공할 필요는 없다.</p>	GDPR의 컨트롤러는 처리의 목적과 수단을 규정하는 역할을 하며, 반드시 정보의 처리를 위탁할 필요는 없음

수탁자	프로세서
<p>[제26조제2항] 수탁자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 의미한다.</p>	<p>[제8조] 프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 개인, 법인, 정부부처 및 관련 기관, 기타단체 등을 의미하며, 컨트롤러의 지시에 따라 개인정보를 처리한다.</p>
개인정보 보호책임자	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. 기업주 또는 대표자</p> <p>나. 임원(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) 컨트롤러나 프로세서, 그리고 데이터 처리를 수행하는 해당 직원에게 GDPR과 EU 또는 회원국의 개인정보보호 조문에 따른 의무에 대하여 고지하고 조언</p> <p>(b) GDPR과 EU 또는 회원국의 개인정보보호 조문에 대한 컨트롤러 또는 프로세서의 정책 준수 여부를 모니터링(직원 교육과 감시 활동 포함)</p> <p>(c) 요청이 있을 경우, 개인정보 영향평가에 관한 자문을 제공하고 평가 이행 상황을 감시</p> <p>(d) 감독기구와의 협력</p> <p>(e) 사전협의 등 처리에 관련된 사항에 대한 감독기구의 연락처 역할을 수행하며, 적절한 경우에는 기타 사안에 대한 자문을 제공</p>

국내법상 개인정보 보호책임자의 자격 요건은 공무원 또는 사업주, 대표자, 임원 등 일정 지위로 구분 하나, GDPR 상 DPO는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 제39조에 언급된 직무를 완수할 능력에 근거하여 지정되어야 함

+ 더 알아보기 / 2

가명처리(Pseudonymisation)

#1 가명처리

GDPR은 정보주체의 위험을 감소시키고 컨트롤러와 프로세서의 의무를 충족시키는 보호조치 중 하나로서 가명처리(pseudonymisation)를 제시하고 있다. 가명처리는 데이터 세트(data set)의 전체나 일부를 가상의 이름이나 부호로 대체함으로써 개인 식별 가능성을 낮추는 데이터의 처리를 의미한다.

※ 다만 데이터 세트(data set)의 익명처리 여부는 △연결 가능성(linkability), △추론(inference) 가능성, △특정(singling out) 가능성 여부를 종합적으로 고려해야 함⁹

다만 전문 제26항에서 가명처리된 정보는 추가적 정보를 이용하여 개인을 식별할 수 있는 정보이므로 식별 가능한 ‘개인정보’로 보아야 한다고 명시하고 있다.¹⁰

#2 가명처리의 활용

가명처리는 개인정보를 처리할 때 위험성을 감소시키는 보호조치의 하나로, 정보주체에 미치는 위험성을 줄이고 컨트롤러와 프로세서의 개인정보보호 의무 준수를 위한 수단으로 활용할 수 있다.

그 예로 GDPR 제25조(Data protection by design and default)에서는 개인정보 처리 방법 결정 시점 및 처리 당시 시점에서 가명처리를 포함한 안전 조치를 취해야 함을 규정한다.

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

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 명시한다.

9 Data Protection Commission, Guidance on Anonymisation and Pseudonymisation, 2019. 06.
10 이와 관련하여 제29조 작업반은 가명처리된 정보의 경우 개인 식별 가능성이 있으므로 데이터 보호를 위한 법적 체제의 범위 내에 들어야 한다는 의견을 밝히고 있다(제29조 작업반, Opinion 05/2014 on Anonymisation Techniques, 2014. 05., p.10.).

#3 가명처리된 정보의 활용

GDPR은 제6조제4항을 통하여 개인정보 처리의 당초 목적과 양립가능성 여부를 판단하는 보호조치 중 하나로 가명처리를 지목하고 있다.

특히 전문 제50항 및 제156항은 공익을 위한 기록 보존의 목적, 과학이나 역사적 연구의 목적, 또는 통계 목적인 경우의 정보 처리는 당초 목적과 양립가능성이 있는 것으로 보고 가명처리를 통하여 추가적인 개인정보 처리가 가능하다고 밝히고 있다. 다만 이러한 경우 추가적 정보는 제4조제5항에 따라 기술적·관리적 조치 하에 별도 분리 보관되어야 한다.



GDPR의 적용 대상과 범위



Point

- GDPR의 적용을 받는 개인정보를 구분할 수 있다.
- GDPR이 적용되는 물적 범위와 장소적 범위를 이해할 수 있다.

4.1 적용 대상(제1조)

4.1.1 어떤 정보에 적용되는지

- GDPR은 개인정보 처리에 대하여 적용된다. GDPR은 관례 및 개별법 등을 통해 표명되어 온 개인정보의 개념을 조문에 포함함으로써 적용 대상을 보다 구체적으로 명시하고 있다. 특히 추가 정보를 이용하여 개인을 식별할 수 있는 가명 정보는 개인정보로 본다는 점을 명확히 하였다(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.

4.1.2 개인정보 보호의 대상은 누구인지

- GDPR은 정보주체인 ‘살아 있는 자연인’의 개인정보에 국한되며, 국적이나 거주지에 관계없이 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).

4.1.3 개인정보의 처리와 관련하여 누가 GDPR을 준수하여야 하는지

- GDPR은 컨트롤러와 프로세서가 개인정보를 처리할 때 적용되며, 컨트롤러뿐만 아니라 프로세서도 GDPR에 규정된 다양한 의무를 준수하여야 한다.



셀프 체크리스트

Self Check List

우리는 컨트롤러(controller)인가?	예	아니오
• 개인정보를 수집하거나 처리하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리의 목적이나 결과를 결정하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보의 수집 여부를 결정하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 어떠한 정보주체의 개인정보를 수집할 것인가를 결정하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 다른 컨트롤러로부터 제공되는 서비스에 대한 결제를 위한 경우를 제외하고, 개인정보의 처리로부터 상업적인 이득이나 기타 이익을 얻는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체와의 사이에 계약의 결과로서 개인정보를 처리하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리의 일부 또는 결과로서 관련된 개인에 대한 결정을 하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체와 직접적인 관계를 가지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보가 처리되는 방법에 관한 완전한 자율성을 가지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 우리를 위하여 개인정보를 처리하는 프로세서를 지명하는가?	<input type="checkbox"/>	<input type="checkbox"/>



셀프 체크리스트

Self Check List

우리는 공동 컨트롤러(joint controller)인가?	예	아니오
• 처리와 관련하여 제3자와 공동의 목적을 가지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 다른 컨트롤러와 동일한 목적을 위하여 개인정보를 처리 하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 다른 컨트롤러와 해당 개인정보 처리를 위한 동일한 데이터 세트(예, 하나의 데이터베이스)를 이용 하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 다른 컨트롤러와 함께 해당 처리를 디자인 하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 다른 컨트롤러와 공동의 정보 관리 규칙을 가지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>



셀프 체크리스트

Self Check List

우리는 프로세서(processor)인가?	예	아니오
• 개인정보의 처리와 관련하여 제3자의 지시를 따르는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 우리는 고객 또는 그와 유사한 제3자로부터 개인정보를 받거나 무슨 개인정보를 수집할 것인가를 알게 되는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인으로부터 개인정보를 수집하는 것을 결정하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 무슨 정보가 개인으로부터 수집되어야 하는지 컨트롤러로부터 지시 받는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 해당 정보의 이용을 위한 법적 근거를 결정하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 해당 정보가 이용될 목적을 결정하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보를 공개할 것인지 또는 누구에게 공개할 것인지를 결정하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 얼마 동안 해당 정보를 보유할 것인지를 결정하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보가 어떻게 처리되는가에 대하여 일부 결정할 수 있지만, 제3자와의 계약에 따라 그러한 결정을 수행하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 처리의 최종 결과에 대하여 관심이 없는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.2 적용 범위

4.2.1 물적 범위(Material scope)(제2조제1항)

- GDPR은 전체 또는 부분적으로 자동화된 수단에 의한 개인정보의 처리에 적용된다 (전자적 데이터베이스나 컴퓨터로 운영되는 파일링시스템 등).
다만, 수기 처리(manual processing)와 같이 비자동화 수단에 의한 개인정보 처리라고 하더라도(관련성 있는)파일링시스템의 일부를 구성하는 경우 등에는 적용 대상이 된다.

4.2.2 장소적 범위(Territorial scope)

- <EU 역내: EU에 사업장을 운영하며, 해당 사업장이 개인정보 처리를 수반하는 경우 (제3조제1항)>
컨트롤러 또는 프로세서가 EU에 사업장(establishment)을 가지고 있고, 해당 사업장에서의 활동이 개인정보의 처리를 포함한다면 GDPR이 적용된다.
전문 제22항에 따를 때, 사업장이란 지속적인 배치(stable arrangements)를 통하여 효과적이고 실제적인 활동(effective and real exercise of activity)을 수행하는 것을 의미한다. 이러한 의미에서 사업장의 설립 형태는 지사(branch)든 법인격을 지닌 자회사(subsidiary)든 상관없다.

⇒ 사례

한국에 본사를 둔 휴대폰 제조회사는 전 지분을 소유한 지사와 사무실이 브뤼셀에 있으며 EU 역내 마케팅 및 광고 등의 운영을 관리하는 업무를 수행한다.

이 지사의 경우에 휴대폰 제조회사가 수행하는 경제 활동의 본질에 비취볼 때 실질적이며 효과적인 활동을 행사하기 때문에 GDPR 의미 내에서 EU 역내 사업장으로 간주할 수 있다.

⇒ 사례

전자상거래 웹사이트를 운영하는 한국회사는 EU시장에 대한 영업 전망 및 마케팅 캠페인을 주도하고 실행할 목적으로 베를린에 유럽 사무소를 개설했다. 정보처리 활동은 한국에서 독점적으로 하는 웹사이트이다. 이 경우 EU시장에 대한 영업 전망 및 마케팅 캠페인 덕분에 전자상거래 웹사이트 서비스가 명백히 수익 창출 역할을 할 경우, 베를린 내 유럽 사무소 활동은 한국 전자상거래 웹사이트가 수행하는 개인정보 처리와 불가분하게 연계된 것으로 간주한다. 한국 회사의 개인정보 처리는 EU 역내 사업장인 유럽 사무소 활동에서 수행되는 것으로 간주되므로 제3조(1)항에 따라 GDPR 조항의 적용을 받는다.

- EU 역내에 사무소, 대리인 또는 지속적인 배치(stable arrangements)를 두지 않은 때에는 GDPR 제3조제1항의 적용을 받지 않는다.

⇒ 사례

한국의 호텔·리조트 체인은 영국, 독일, 프랑스 및 스페인에서 사용할 수 있는 패키지를 웹사이트를 통해 제공하지만, EU 역내에 사무소, 대리인 또는 지속적인 배치를 두고 있지 않다. 호텔·리조트의 대리인 및 지속적인 배치가 EU 역내에 없을 경우에 GDPR 제3조제1항 적용 측면에서는 EU 사업장으로서 자격 요건이 성립될 수 없고, 따라서 관련된 처리는 GDPR 제3조제1항에 따른 적용을 받지 않는다. 그러나 한국의 호텔·리조트 체인의 구체적인 활동을 분석함으로써 GDPR 제3조제2항에 따른 적용을 받을 여지는 남아 있다.

- <EU 역외: EU에 있는 정보주체에게 재화나 서비스를 제공하는 경우 또는 EU 내 정보주체의 행동에 대한 모니터링(제3조제2항)>
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.

⇒ 사례

EU 역내에 영업 실체나 사업장이 없는 한국 스타트업이 관광객을 대상으로 지도 서비스 앱을 제공한다. 관광객이 앱을 사용하면 정보주체인 고객의 위치에 대한 개인정보를 처리하여 방문 장소, 식당, 쇼핑물 및 호텔에 대한 맞춤형 광고를 제공한다. 뉴욕, 샌프란시스코, 토론토, 런던, 파리와 로마 방문객이 사용할 수 있다. 이 기업은 지도앱으로 EU 회원국인 파리와 로마에서 서비스를 제공한다.

결국 서비스 제공과 관련하여 EU 회원국 정보주체의 개인정보를 처리하는 것은 제3조제2항에 따라 GDPR의 적용대상이 된다.

② EU 내에 있는 정보주체에 대하여 EU 내에서의 행동을 모니터링하는 경우

⇒ 사례

한국에서 설립된 마케팅 회사는 몰타 쇼핑 센터에게 유통 배치(retail layout)에 대한 자문을 제공한다. 와이파이 추적으로 수집된 센터 내 고객 동선을 분석함으로써 가능하다. 와이파이 추적을 이용한 센터 내 고객 동선 분석은 개인정보 모니터링이다. 이 경우 쇼핑 센터가 몰타에 있기 때문에 정보주체의 행동이 EU 내에서 발생한다. 컨트롤러로서 한국의 마케팅 회사는 제3조제2항(b)에 따라 정보 처리 측면에서 GDPR의 적용을 받는다. 또한 GDPR 제27조에 따라 컨트롤러인 한국의 마케팅 회사는 EU 내에 대리인(representative)을 지정하여야 한다.

4.3 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 형사처벌 집행 관련 활동

GDPR 관련 규정	<ul style="list-style-type: none">■ 제4조(정의)■ 제2조(물적 범위)■ 제3조(장소적 범위)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제2조(정의)



02

개인정보
처리기준



1. 개인정보 처리 원칙
2. 처리의 합법성(Lawfulness of processing)(제6조)
3. 동의(Consent)(제7조)
4. 아동 개인정보(Children's personal data)(제8조)
5. 민감정보 및 범죄정보(Special categories of personal data
& Personal data relating to criminal convictions and
offences)(제9조, 제10조)



개인정보 처리 원칙



Point

- 개인정보를 처리할 때 준수하여야 하는 7가지 기본 원칙을 이해할 수 있다.
- 이 원칙을 위반할 경우 과징금이 부과될 수 있다.

개인정보 처리 원칙

합법성, 공정성, 투명성	개인정보는 정보주체와 관련하여 합법적이고, 공정하며, 투명한 방식으로 처리되어야 한다.
목적 제한	개인정보는 특정되고 명시적이며 적법한 목적으로 수집되어야 하며, 그러한 목적과 양립하지 않는 방식으로 처리되지 말아야 한다.
최소처리	개인정보는 처리되는 목적과 관련하여 적당하고 관련성이 있으며 필요한 범위로 제한되어야 한다.
정확성	개인정보는 정확해야 하고, 필요한 경우 최신성을 유지해야 한다.
보유기간의 제한	개인정보는 처리목적을 위해서 필요한 기간 내에서 정보주체를 식별할 수 있는 형태로 보유되어야 한다.
무결성 및 기밀성	개인정보는 적절한 기술적 또는 관리적 조치를 이용하여 개인정보의 적절한 보안을 보장하는 방식으로 처리되어야 한다.
책임성	컨트롤러는 개인정보보호원칙에 대하여 책임성을 갖춰야 하며, 그에 대한 준수 여부를 증명할 수 있어야 한다.

1.1 합법성·공정성·투명성의 원칙



셀프 체크리스트

Self Check List

	예	아니오
합법성		
• 개인정보 처리 시 적법한 근거를 제시하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 민감정보·범죄정보 처리 관련 조건을 확인했는가?	<input type="checkbox"/>	<input type="checkbox"/>
공정성		
• 귀사의 개인정보 처리가 정보주체에게 어떤 영향을 미치는지 고려하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 부정적 영향을 미치는 경우 타당한 근거가 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
투명성		
• 개인정보 처리 정책의 접근이 용이하며 명확하고 쉬운 언어가 사용되었나?	<input type="checkbox"/>	<input type="checkbox"/>

1.1.1 합법성

- ‘합법성(lawfulness)’이란 개인정보 처리가 합법적이라는 것을 의미한다. 개인정보 처리가 합법적인 것으로 인정받기 위해서는 처리를 위한 구체적인 근거를 제시해야 한다. GDPR은 개인정보 처리의 합법적 근거를 제6조(처리의 적법성), 제7조(동의의 조건), 제9조(민감정보), 제10조(범죄정보)에서 상세히 규정하고 있다.
- 일반 개인정보의 합법적 처리를 위한 6가지 조건(제6조) 이외에 민감정보 및 범죄정보의 합법적 처리를 위한 추가 조건을 규정하고 있고(제9조, 제10조), 유효한 “동의”가 되기 위한 조건을 별도로 규정하고 있다(제7조).

개인정보 처리와 관련해서 앞에서 설명한 합법적인 근거 중 하나를 제시하지 못하면 그 처리는 불법적인 것이 되어 합법성 원칙을 위반하게 된다.

보다 넓은 의미에서 합법성은 민·형법을 비롯한 각종 법령이나 계약상의 의무를 위반하지 않는다는 것을 의미하기도 한다. 그와 같은 위반의 예로는 다음과 같은 것이 있다.

- ① 비밀유지의무 위반
- ② 권한 남용 또는 권한의 부적절한 행사
- ③ 저작권 침해

- ④ 계약 위반
- ④ 산업별 개별법규 위반
- ⑤ 인권법 위반
- 그러나 이와 같은 불법적인 개인정보 처리가 모두 GDPR의 적용 대상은 아니며 감독기구가 다룰 수 있는 업무도 아니다.
개인정보를 불법으로 처리한 경우 GDPR은 정보주체에게 해당 개인정보를 삭제하거나 처리를 제한할 수 있는 권한을 부여하고 있다.

1.1.2 공정성

- ‘공정성(fairness)’이란 사람들이 합리적으로 기대할 수 있는 방식으로 개인정보를 처리하고 정보주체에게 부당한 영향을 미치는 방식으로 개인정보를 이용하지 않는다는 것을 의미한다.
- 첫째, 공정한 처리가 되기 위해서는 개인정보의 수집 방법이 합리적이어야 한다. 누군가를 속이거나 부정한 방법으로 개인정보를 수집했다면 공정한 처리라고 할 수 없다.
- 둘째, 개인정보 처리가 공정한지 여부를 평가할 때에는 정보주체에게 미치는 영향을 고려해야 한다. 수집·이용 방법이 대다수 사람들에게 공정하더라도 특정 개인에게 불공평하다면 공정성 원칙 위반이 될 수 있다. 다만, 개인정보가 특정 개인에게 불이익한 영향을 미치는 방식으로 처리되었더라도 그 처리 과정이 불공평하지 않으면 불공정한 처리라고 할 수 없다. 그런 경우에는 그 불이익이 정당한 것인지 여부를 따져 보아야 한다. 예컨대 세금 부과, 속도위반에 대한 과태료 처분 등을 위한 개인정보 처리는 정당하다.
- 셋째, 개인정보 ‘처리’에 대한 합법적인 근거를 입증할 수 있는 경우라도 개인정보 처리 ‘방법’이 공정하지 않으면 개인정보 처리원칙을 위반한 것이 될 수 있다.

1.1.3 투명성

- ‘투명성(transparency)’이란 개인정보를 누가, 어떤 목적으로, 어떤 정보를, 어떤 방식으로 처리하는지를 명확하게 알리는 것을 의미한다. 그와 같은 정보는 (1) 정보주체가 쉽게 접근할 수 있고, (2) 간결하며 (3) 평이한 언어를 사용하여, (4) 이해하기 쉬운 방식으로 제공되어야 한다. 따라서 투명성은 공정성과도 밀접한 관련이 있다.
투명성 원칙은 정보주체로부터 개인정보를 직접 수집할 때도 중요하지만 정보주체 이외로부터 수집할 때 더 중요하다. 정보주체가 개인정보 처리 사실을 모르면 권리행사

를 할 수 없기 때문이다. 이에 따라 GDPR은 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식), 제13조(정보를 제공받을 권리), 제14조(정보를 제공받을 권리), 제15조(정보주체의 접근권)에서 투명성 원칙을 실현하기 위한 구체적인 방법을 규정하고 있다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제5조(개인정보 처리 원칙)(1)(a) ■ 제6조(처리의 합법성) ■ 제9조(민감정보) ■ 제10조(범죄정보의 처리) ■ 제13조 및 제14조(정보를 제공받을 권리) ■ 제17조(삭제를 요구할 권리) ■ 전문 제39항 ■ Guidelines on transparency under regulations 2016/679, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제22조(동의를 받는 방법) ■ 제30조(개인정보처리방침의 수립 및 공개)

1.2 목적 제한의 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보 처리 목적을 구체적으로 제시하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 처리 목적을 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 처리활동을 정기적으로 검토하고 필요할 경우 개인정보보호 정책을 업데이트 하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 새로운 목적으로 개인정보 이용 시 본래 목적과 양립하는지 또는 새 목적 관련 구체적인 동의를 얻었는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.2.1 목적 제한의 원칙이란?

- 목적 제한(purpose limitation)의 원칙은 개인정보를 수집할 때 처음부터 개인정보의 처리 목적을 구체적이고 명시적으로 제시해야 하고, 적법한 목적을 위해서 수집해야 하며, 최초 수집 목적과 부합하지 않는 방식의 추가 처리를 하지 않는다는 원칙이다. 목적 제한의 원칙을 준수하기 위해서는 다음의 사항을 고려해야 한다.

첫째, 개인정보를 수집하는 이유와 수집한 개인정보로 무엇을 할 것인지 처음부터 명확히 해야 한다.

둘째, 목적을 명확화하기 위하여 문서화해야 한다.

셋째, 정보주체에게 목적을 투명하게 알려야 한다.

넷째, 원래의 목적과 다른 목적으로 개인정보를 이용하거나 제공하려는 경우 그 목적은 공정하고 합법적이며 투명해야 한다. 다만 공익을 위한 기록 보존 목적, 과학적·역사적 연구 목적 또는 통계 목적을 위한 개인정보의 추가 처리는 가명처리 등 안전한 조치를 취하는 한 원래 목적과 양립 가능한 것으로 본다.

1.2.2 목적 제한의 필요성

- 목적 제한의 원칙은 개인정보의 수집 이유를 명확히 공개하고, 개인정보의 처리를 공개된 목적으로 제한함으로써 개인정보의 처리 활동이 정보주체의 합리적인 기대와 일치하게 하는 것을 목적으로 한다.
- 처음부터 처리 목적을 명확히 해두면 개인정보의 처리에 대한 컨트롤러의 책임감을 높이고 컨트롤러가 은연중에 처리 목적을 확대하는 것을 막을 수 있다. 또한 정보주체는 컨트롤러가 개인정보를 어떻게 이용할지 이해할 수 있고, 개인정보 처리에 대한 동의 여부를 결정하는 등 정보주체의 권리 행사에도 도움을 준다.
- 목적제한은 합법성, 공정성, 투명성 원칙과도 관련이 있다. 개인정보의 처리 이유를 명확히 하면 처리가 공정하고 합법적이며 투명하다고 할 수 있기 때문이다.
따라서 개인정보를 불공정하거나 불법적, 혹은 은닉을 목적으로 이용하면 목적 제한 원칙과 합법성, 공정성, 투명성 원칙을 둘 다 위반한 것이 될 수 있다.

1.2.3 목적 명시 방법

- 처리 목적을 문서화하고 투명성 의무를 준수하는 것만으로도 다른 추가적인 조치 없이 목적 명시 의무를 준수할 수 있다. 즉, GDPR 제30조에 따른 처리 활동 기록·관리의 의무 일부로 보관이 요구되는 문서에 처리 목적을 명시하고, 제13조 및 제14조에 따라

정보주체에게 제공되어야 할 필수고지 사항에 처리 목적을 구체화하면 목적 명시 의무를 준수한 것이 된다. 소규모 조직으로서 문서화 요구 의무가 면제된 경우에는 목적 제한 원칙을 준수하기 위해 모든 목적을 “공식적으로” 문서화할 필요는 없다. 정보주체에게 제공하는 고지사항에 처리 목적을 기재하는 것으로도 충분하다. 그럼에도 불구하고 모든 목적을 문서화하는 것이 여전히 바람직하다. 정보주체가 이미 알고 있는 목적으로만 개인정보를 처리하여 고지 의무를 이행할 필요가 없는 경우라면 그 목적은 분명하고 구체화 되어 있어야 한다. 또한, 컨트롤러는 처리 목적이 최초 수집 시 명시한 목적을 넘어서 처리되고 있는지 여부를 확인하기 위하여 개인정보의 처리현황, 관련 문서, 고지사항 등을 정기적으로 검토해야 한다. 위와 같이 컨트롤러가 처리 목적을 문서화하고 정보주체에 대한 고지 의무를 준수했다고 해서 근본적으로 불공정한 처리를 공정하고 합법적인 처리로 만들 수는 없다.

1.2.4 개인정보의 목적 외 이용

- GDPR은 개인정보의 목적 외 이용을 완전히 금지하지는 않지만 제한을 두고 있다. 개인정보의 목적 외 이용은 다음 중 어느 하나에 해당하는 경우에만 가능하다.
 - 새로운 목적이 원래의 목적과 양립 가능한 경우
 - 새로운 목적에 대하여 정보주체로부터 구체적인 동의를 받은 경우
 - 공익을 위하여 새로운 목적의 처리를 요구하거나 허용하는 명확한 법률 조항을 제시할 수 있는 경우
- 새로운 목적이 양립 가능한 경우 추가 처리를 위하여 새로운 처리 근거가 필요하지는 않지만, 원래의 동의를 기반으로 개인정보를 수집한 경우에는 일반적으로 새로운 처리가 공정하고 합법적인 것임을 보장하기 위하여 새로운 동의를 받아야 한다. 또한 처리 목적이 바뀐 경우에는 개인정보 처리의 투명성을 보장하기 위하여 정보주체에 대한 고지사항도 현행화해 두어야 한다.

1.2.5 양립 가능한 목적이란?

- GDPR은 특별히 ① 공익을 위한 기록 보존 목적, ② 과학적·역사적 연구 목적, ③ 통계 목적을 위한 개인정보의 추가 처리는 원래의 목적과 양립이 가능한 것으로 규정하고 있다. 위의 목적이 아니라면, 새로운 목적이 원래의 목적과 양립 가능한지 여부를 결정하기 위해서는 아래와 같은 사항을 고려해야 한다고 규정하고 있다(제6조제4항, 전문 제50항).
 - 원래의 목적과 새로운 목적의 연관성

- 정보주체와의 관계, 양 당사자의 합리적인 기대 등 처음 개인정보를 수집할 때의 상황
 - 민감정보인지 여부 등 개인정보의 성격
 - 새로운 개인정보 처리가 정보주체에게 미칠 결과
 - 암호화, 가명처리 등 적절한 보호 수단의 유무
- 일반적으로 새로운 목적이 원래 목적과 매우 다르거나, 예상하기 어렵거나, 정보주체에게 부당한 영향을 미치는 경우에는 원래 목적과 양립하지 않는다. 이 경우 개인정보를 이용 또는 제공하려면 정보주체의 구체적인 동의를 받아야 한다. 양립 가능한 목적은 합법성, 공정성 및 투명성 원칙과도 관련이 있다. 의도한 개인정보 처리가 공정하다면 양립성 원칙에 따라 목적 제한 원칙을 위반하지 않을 수 있다.

⇒ 사례

개업 의사인 남편이 회복이 필요한 환자에게 휴가 여행 권유를 위하여 여행을 운영하는 아내에게 자신의 환자 목록을 제공하였다. 이 목록을 이용하여 아내는 치료가 필요한 환자들에게 의료 관광 할인 상품을 제안하고자 한다. 이와 같은 목적을 위한 개인정보의 제공은 수집 시의 목적과 양립한다고 볼 수 없다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제5조(개인정보 처리 원칙)제1항(b)■ 제6조(처리의 합법성)제4항■ 제30조(처리활동의 기록)■ 전문 제39항, 제50항■ Guidelines on transparency under regulations 2016/679, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제3조(개인정보보호 원칙)■ 제15조(개인정보의 수집·이용)■ 제17조(개인정보의 제공)■ 제18조(개인정보의 목적 외 이용·제공 제한)■ 제19조(개인정보를 제공받은 자의 이용·제공 제한)■ 제28조의2 가명정보의 처리 등■ 제28조의3 가명정보의 결합 제한■ 제28조의4 가명정보에 대한 안전조치의무 등■ 제28조의5 가명정보 처리 시 금지의무 등■ 제28조의6 가명정보 처리에 대한 과징금 부과 등■ 제28조의7 적용범위

1.3 개인정보 최소화처리 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 명시된 목적에 실제로 필요한 정보만 수집하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보유 개인정보를 정기적으로 검토하고 필요 없는 정보를 삭제하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.3.1 최소화처리 원칙이란?

- ‘최소처리(data minimisation)’ 원칙이란 처리 목적을 달성하기 위하여 적절한 범위 내에서, 처리 목적과 합리적으로 관련이 있고, 목적을 달성하기 위하여 필요한 것 이상으로 처리하지 않는다는 원칙이다.

최소처리 원칙은 정확성 원칙, 보유기간 제한 원칙과 함께 “개인정보 처리 표준”에 관한 세 가지 원칙 중 첫 번째 원칙에 해당한다.

- 컨트롤러는 목적 달성에 필요한 최소한의 개인정보를 파악하고, 그 범위 내의 개인정보만 가지고 있어야 하며, 그 이상의 개인정보를 가지고 있어서는 안 된다.

또한, 컨트롤러는 목적 달성에 필요한 개인정보만 수집해서 보유할 것임을 보장하기 위한 적절한 프로세스를 갖추고 있다는 것도 증명해야 한다.

정보주체는 목적 달성에 적합하지 않은 불완전한 개인정보의 정정·보완을 요구할 수 있고, 목적 달성에 필요하지 않은 개인정보의 삭제를 요구할 수도 있다.

1.3.2 적정성, 관련성 및 제한성

- 최소화처리 원칙 준수를 위해서는 목적 달성에 적합한 개인정보만을 처리해야 한다. 개인정보 처리가 목적달성에 부합하는지를 판단하기 위해서는 처리의 적정성, 관련성, 제한성을 고려해야 한다. GDPR은 이들 용어에 대한 정의를 두고 있지 않지만, 일반적으로 ‘적정성(adequate)’이란 처리 목적을 달성하기 위하여 요구되는 정도를 의미하고, ‘관련성(relevant)’은 처리 목적과 합리적으로 관련이 있어야 한다는 것을 의미하며, ‘제한성(limited)’은 처리 목적 달성에 필요한 이상으로 보유하고 있어서는 안 된다는 것을 의미한다.

따라서 개인정보를 수집하고 이용하는 목적에 따라 그 범위는 다를 수 있고, 또한 개인정보를 처리하는 상황에 따라 달라질 수 있다.

적정한 양의 개인정보를 보유하고 있는지 여부를 평가하기 위해서는 먼저 그 정보가 필요한 이유를 명확히 설명할 수 있어야 한다.

특히 민감정보와 범죄정보의 경우 최소한의 정보만 수집하고 보유하도록 하는 것이 매우 중요하다.

- 컨트롤러는 정보주체별로 또는 관련 특성을 공유하는 정보주체의 그룹별로 각각 적정성, 관련성 및 제한성을 고려해야 한다. 특히 정보주체가 정정권 또는 삭제권을 행사한 경우에는 그 사유도 고려해야 한다.

끝으로, 개인정보 처리 현황을 정기적으로 검토하여 보유하고 있는 개인정보가 여전히 처리 목적에 적절하고 관련이 있는지 여부를 확인하고 더 이상 필요하지 않은 개인정보는 삭제해야 한다. 이는 보유기간 제한 원칙과 밀접한 관련이 있다.

1.3.3 과도한 개인정보의 처리 금지

- 컨트롤러는 원칙적으로 목적 달성을 위해 필요한 것 이상의 개인정보를 보유해서는 안 되고, 목적 달성과 관련이 없는 세부사항을 포함해서도 안 된다.

특정 채무자를 찾기 위해 고용된 채권추심회사는 채무자와 이름이 비슷한 여러 사람에 관한 정보를 수집해야 하는 경우가 있는데 조사 과정에서 이들 중 일부는 조사 대상에서 제외되기도 한다.

이 때 조사 대상에서 제외된 사람의 개인정보는 최소한의 기본적인 사항만 보유하고 대부분의 개인정보는 삭제해야 한다. 정보주체가 자신과 관련이 없는 채무와 관련해서 다시 연락을 받지 않도록 최소한의 정보만 보유해야 한다.

특히 특정 개인에 관한 정보만 처리할 필요가 있는 경우에는 그 개인에 관한 정보를 수집해야 한다.

⇒ 사례

채용대행 회사는 일반적으로 지원자들을 다양한 직무에 배치한다. 채용 대행을 위해 대행회사는 신청자들에게 통상적으로 설문지를 보내는데 해당 설문지에는 특정 직무에만 관련이 있는 건강 상태에 관한 질문이 포함되어 있을 수 있다. 사무직에 지원한 신청자에게 그와 같은 건강정보를 수집하는 것은 무관하고 과도하다.

장래에 유용할 지도 모른다는 막연한 기대를 가지고 개인정보를 수집해서도 안 된다. 다만, 그것을 정당화할 수 있다면 개인정보를 보유할 수 있다.

⇒ 사례

기업은 만일의 사고에 대비하여 위험한 일에 종사하고 있는 일부 근로자들에 대한 혈액형 정보를 보유할 수 있다. 사고 예방을 위한 안전절차를 시행하고 있어 혈액형 정보가 필요하지 않을 수 있으나 비상시에는 여전히 해당 정보를 보유할 필요가 있다. 그러나 위험한 일에 종사하고 있지 않은 다른 직원의 혈액형 정보는 목적과 관련성이 없기 때문에 기업이 해당 정보를 처리하는 것은 과도하다.

그러므로 목적 달성을 위해 실제로 필요한 것보다 많은 개인정보를 보유하고 있다면 불법일 가능성이 높고 개인정보 최소처리 원칙을 위반할 수 있다.

1.3.4 부적절한 개인정보의 처리 금지

- 해당 개인정보의 처리가 목적 달성에 필요하지 않다면, 그 개인정보는 부적절한 정보이다. 개인정보가 수집 시 의도한 목적에 부적절한 경우 처리해서는 안 된다. 다만, 어떤 상황에서는 목적 달성을 위하여 처음에 예상한 것보다 더 많은 개인정보를 수집해야 하는 경우도 있을 수 있다.

⇒ 사례

처음 모임을 구성할 때에는 회원수가 적고 회원 간에 서로를 잘 알고 있어서 회원의 이름과 이메일 주소만으로 모임 운영이 가능했다. 그러나 모임이 인기가 있어 회원 수가 빠르게 증가할 경우 회원의 신원을 제대로 파악할 수 있도록 하고 회원가입 여부, 회비납부 현황 등을 확인할 수 있도록 회원에 관한 추가 정보를 수집할 필요가 있다.

- 또한, 사실에 대한 불완전한 이해에 근거해서 누군가에 대한 결정을 내린다면 그 같은 결정에 이용된 개인정보는 부적절한 것일 수 있다. 특히 정보주체가 정정권에 따라 불완전한 정보의 보완·정정을 요구해 온 경우 이는 곧 해당 정보가 목적 달성에 부적절한 것임을 의미할 수 있다.

1.3.5 정보주체에 관한 ‘의견’ 정보 기록의 적정성과 관련성

- ‘의견’에 관한 정보가 기록되어 있는 경우에 정보주체가 기록에 동의하지 않았거나 정보주체가 중요하다고 생각하는 정보를 고려하지 않았다고 해서 반드시 그 기록이 부적절하거나 관련성이 없는 것은 아니다.

그러나 의견의 기록이 적절한 것이 되기 위해서는 그 기록이 사실이 아니라 의견이라는 것을 분명히 해야 한다.

- 또한 의견의 기록에는 독자가 그것을 정확하게 이해할 수 있도록 충분한 관련 정보가 포함되어 있어야 한다. 예를 들어 작성 일자, 작성자의 이름과 직위를 명시해야 한다. 어떤 의견이 논란이 되거나 매우 민감할 가능성이 있는 경우, 또는 이용·공개될 때 중대한 영향을 미칠 경우에는 그 의견의 근거나 정황을 진술해 두는 것이 더욱 중요하다. 또한, 기록이 다른 곳에 보관된 상세한 기록을 요약한 것이라면 기록에 이 점을 분명히 밝혀야 한다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제5조(개인정보 처리 원칙) 제1항(c) ■ 제16조(정정권) ■ 제17조(삭제권) ■ 전문 제39항 ■ Guidelines on transparency under regulations 2016/679, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제16조(개인정보의 수집 제한) ■ 제22조(동의를 받는 방법)

1.4 정확성 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 모든 개인정보의 정확성을 보장하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보의 출처기록을 포함하여 정확성을 보장하기 위한 프로세스를 갖추었는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정정·삭제권과 이의제기권을 보장하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보를 업데이트할 시점을 파악하기 위한 프로세스를 갖추었는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.4.1 정확성 원칙이란?

- 정확성(accuracy) 원칙이란 개인정보 처리는 정확해야 하고, 필요시 처리되는 개인정보는 최신의 상태로 유지되어야 한다는 원칙이다. 이에 따라 정확성 원칙은 개인정보 정정·삭제 요구권과도 밀접한 관계를 가진다.

정확성 원칙은 개인정보 최소화처리 원칙, 보유기간 제한의 원칙 등과 함께 개인정보 처리 표준에 관한 3대 원칙 중 두 번째 원칙이다. 정확성 원칙을 준수하기 위해 컨트롤러는 처리 목적에 비추어 부정확하거나 오해의 소지가 있는 개인정보의 즉각적인 삭제 또는 정정을 보장하기 위한 모든 합리적 조치를 취해야 한다. 또한, 개인정보의 출처와 중요도를 명확히 파악·관리해야 하고, 정확성에 대해 이의제기가 있는 경우에는 신중하게 검토하여야 하며, 필요하다면 개인정보를 정기적으로 업데이트해야 한다.

- 다만, 컨트롤러는 필요시 개인정보를 업데이트할 수도 있고 또는 업데이트해야 하지만, 이는 개인정보의 처리 목적에 따라 달라질 수 있다. 즉, 목적에 반해서 업데이트해서는 안 된다.

1.4.2 정확성(Accuracy) 또는 부정확성(Inaccuracy)

- GDPR은 '정확성'에 대한 정의를 두고 있지 않다. 개인정보가 정확한지 여부는 대부분 쉽게 알 수 있기 때문이다. 일반적으로 사실이 아니거나 오해의 소지가 있으면 부정확한 것으로 본다.

- 정확성 여부를 판단하기 위해서는 개인정보를 수집·보유하는 보유 또는 의도를 명확히 해야 한다. 어떤 목적으로 이용하느냐에 따라 그 개인정보가 정확할 수도 있고 부정확할 수도 있다. 정확한 개인정보가 나중에 변경되었다고 해서 그 정보가 항상 부정확해지는 것은 아니다.

⇒ 사례

어떤 사람이 서울에서 인천으로 이사를 했다면 그 사람이 현재 서울에 살고 있다는 기록은 부정확하다. 그러나 그 사람이 한때 서울에 살았다는 기록 그 자체는 정확하다. 따라서 해당 개인정보의 이용 목적에 따라 그 기록은 정확한 것일 수도 있고 부정확한 것일 수도 있다.

1.4.3 오류에 관한 기록의 유지

- 정보주체는 자신에 관한 기록이 불리하게 남아 있는 것을 원하지 않을 수 있다. 예컨대 정보주체가 계약취소로 요금을 환불받은 경우, 그 같은 기록이 남아 있는 것을 원치 않을 수 있다. 그러나 이 경우 요금이 부과되었지만 나중에 취소 및 환불된 사실을 정확히 하기 위해 해당 기록이 합법적으로 필요할 수 있다. 따라서 오류 및 그 정정에 관한 기록을 유지하는 것이 정보주체에게도 이익이 될 수 있다.

⇒ 사례

병원의 오진 기록은 해당 환자에 대한 치료방법을 설명하기 위한 목적이나 다른 건강상의 문제와도 관련이 있을 수 있으므로, 진단서를 수정한 후에도 의료기록의 일부로 계속 보존되어야 한다.

- 그러므로 사실을 오도하거나 오해할 위험이 없다면 오류에 관한 기록도 유지하는 것이 허용된다. 다만, 오류가 있었다는 것을 분명히 하기 위해 그 사유를 추가해야 할 필요성이 있을 수 있다.

⇒ 사례

근로자가 부정행위를 이유로 해고를 당했으나, 노동위원회에서 그 해고는 부당하다는 결정이 내려져 복직 되었다. 근로자는 기업에게 해고 사건과 관련한 모든 정보를 삭제할 것을 요구한다. 그러나 해고 사실에 관한 기록 그 자체는 정확하다. 이 경우 기업은 노동위원회의 부당 해고 결정으로 복직이 되었다는 사실을 기록에 추가해 두어야 한다.

1.4.4 의견의 정확성 문제

- 의견의 기록은 정보주체가 동의하지 않았다고 해서 반드시 부정확하다거나 틀린 것으로 간주되지 않는다. 의견은 본질적으로 주관적이며 사실을 기록하려는 것이 아니다. 그러나 정확성을 기하기 위해서는 해당 기록이 의견이라는 사실을 명확히 밝혀야 하고, 가능하면 누구의 의견인지도 분명히 해야 한다. 또한, 의견이 부정확한 데이터에 기초했다는 것이 명백해지면 그 의견으로 인해 오해의 소지가 없도록 그 이유를 기록해 두어야 한다.

⇒ 사례

의사들이 일상적으로 기록하는 의학적 견해는 매우 민감한 개인정보이다. 환자가 특정 질환으로 고통을 받고 있는지 여부는 시간이 흐르거나 검사가 행해질 때까지는 확실하게 결론을 내리는 것이 불가능한 경우가 많다. 최초의 진단은 보다 광범위한 검사 또는 추가 검사 후에 부정확한 것으로 판명될 수 있다. 그러나 환자에 관한 기록이 특정 시점에 당시 의사의 진단을 정확히 반영하고 있다면 그 기록은 부정확한 것이 아니다. 의사의 초기 진단 기록은 나중에 환자를 치료하는 데 도움이 될 수 있고, 개인정보 최소처리 원칙 중 적정성 요건을 준수하기 위해서도 필요하다.

- 만약 의견의 정확성에 대하여 이의제기가 있다면 그 사실과 이유를 기록해 두는 것이 바람직하다.
어떤 의견에 실제로 얼마나 무게를 두는가는 의견을 기록한 사람의 경험과 신뢰 그리고 그 의견을 기초로 하는 사건에 달려 있다. 짧은 회의 동안 형성된 의견은 깊이 있는 협상을 통해서 도출된 의견보다 비중이 덜할 수 있다. 그러나 이것은 정확성의 문제가 아니라 개인정보 최소처리 원칙에 따른 '적정성'의 문제이므로 그 개인정보가 목적에 적절한지 여부를 검토해야 한다.
- 의견으로 보일 수 있는 기록 중에는 의견이 전혀 포함되어 있지 않는 경우도 있다. 예를 들어, 많은 금융회사는 신용등급을 이용하여 신용 제공 여부를 결정한다. 신용등급은 과거의 신용정보 기록을 통해서 개별 신용을 제공하는데 수반되는 위험을 수치적으로 예측하는 정보다.
- 즉, 신용등급은 개인의 신용도에 대한 주관적인 의견이 아니라 정보주체의 개인정보에 대한 통계적 분석에 기초한다. 그러나 이 경우에도 기초 데이터의 정확성과 적정성을 보장해야 한다.

1.4.5 개인정보의 업데이트

- 컨트롤러는 개인정보를 항상 업데이트해야 하는 것은 아니다. 이는 이용 목적에 따라 달라진다. 이용 목적 달성을 위해 필요하다면 개인정보를 업데이트해야 한다.
예컨대, 급여가 인상되었을 때에는 직원의 급여 기록을 갱신해야 한다. 고객의 주소가 변경되었을 때에는 기록을 업데이트하여 상품이 올바른 장소로 배달되도록 해야 한다.
그러나 목적 달성을 위하여 필요하지 아니한 경우 개인정보를 업데이트할 필요는 없다.

⇒ 사례

정보주체가 일회성 주문을 한 경우에도 사업자는 세무·회계상의 이유와 추후 발생할지 모르는 불만 처리를 위해 일정기간 동안 주문 기록을 보유할 필요가 있다. 그러나 이 경우 사업자는 정보주체가 어디에 살고 있는지 업데이트하거나 정기적으로 확인해야 할 의무는 없다.

- 개인정보의 업데이트가 오히려 개인정보 처리 목적을 훼손한다면 업데이트를 할 필요가 없다. 예를 들어, 통계, 역사, 그 밖의 연구 목적으로만 개인정보를 보유하고 있는 경우 개인정보 업데이트는 그 목적을 훼손할 수 있다.
주소 및 전화번호 같은 정보가 변경된 경우에는 정보주체에게 변경 내용을 알리도록 하는 것이 더 합리적이다. 정보주체에게 정기적으로 자신의 정보를 업데이트 하도록 요구하는 방법도 생각할 수도 있으나, 그것을 정당화 할 수 있을 정도의 필요성이 존재하지 않는 한 최신 기록을 유지하기 위해서 그런 과도한 조치를 요구해서는 안 된다.

⇒ 사례

사업자들의 경우 마케팅 목적을 위해서 과거 고객의 주소와 연락처를 보관하는 경우가 있다. 그러나 해당 기록이 최신 상태인지 여부를 확인하기 위해 데이터 매칭 서비스나 추적 서비스를 이용해서는 안 된다. 그와 같은 목적을 위한 데이터 매칭 또는 추적은 합법성, 공정성 및 투명성 원칙에 부합하지 않기 때문이다.

- 그러나 정보주체가 새로운 주소를 알려 온 경우에는 그 기록을 업데이트하여야 한다. 그리고 주소 불명 등으로 우편물이나 이메일이 반송되어 온 경우에는 해당 연락처가 더 이상 최신 상태가 아님을 표시해 두어야 한다.

1.4.6 정확성 확보를 위한 조치

- 개인정보를 처리 할 때는 해당 정보가 정확한지 여부를 확인해야 한다. 그 정보가 정보 주체에게 심각한 영향을 미칠 수 있는 경우에는 더욱더 주의해야 한다. 예를 들어, 연봉인상과 성과급에 따라 근로자에게 급여를 인상해야 하는 경우 급여기록에서 새로운 급여 수치를 틀리게 기입해서는 안 된다.

다른 사람이 제공하는 개인정보의 정확성을 확인하는 것은 비현실적일 수 있지만, 기록이 부정확하거나 오해를 야기하지 않도록 하기 위해서는 다음과 같은 조치를 취해야 한다.

- 첫째, 제공받은 개인정보를 정확하게 기록해야 한다.
 - 둘째, 정보의 출처를 정확하게 기록해 두어야 한다.
 - 셋째, 정보의 정확성을 확보하기 위해 상황에 따른 합리적인 조치를 취해야 한다.
 - 넷째, 개인정보의 정확성에 대한 모든 이의제기를 주의 깊게 고려해야 한다.
- 무엇이 ‘합리적인 조치’인지는 구체적인 상황, 특히 개인정보의 성격과 그 개인정보를 어떤 목적에 이용할 것인가에 달려 있다. 개인정보의 정확성이 중요할수록 정확성을 확보하기 위해 더 많은 노력을 기울여야 한다.

어떤 사람에게 상당한 영향을 미칠 수 있는 결정을 하기 위해 개인정보를 이용하는 경우 정확성을 확보하기 위해 더 많은 노력을 기울일 필요가 있다. 이는 경우에 따라 개인정보가 정확하다는 것을 추가적으로 확인 받아야 함을 의미할 수도 있다.

예를 들어, 고용주는 특정 업무에 입사지원자의 학력, 자격, 업무경력 등이 필수적이라면 관련 사항을 정확하게 점검하고 검증을 받아야 할 것이다.

⇒ 사례

운전기사를 모집하는 회사는 인터뷰에 응한 지원자가 해당 차량을 운전할 자격이 있는지 여부를 확인해야 한다. 그러나 지원자가 20년 전에 백화점에서 피팅 모델로 근무했다고 자신의 업무경력에 기록해 두고 있는 경우 그 같은 경력은 업무와 관련이 없으므로 굳이 확인할 필요가 없다.

- 개인정보를 제공한 출처가 신뢰할 수 있거나 잘 알려진 조직이라면 일반적으로 정확한 개인정보를 제공했을 것이라고 생각하는 것이 합리적일겠지만, 그런 경우에도 사정에 따라서는 개인정보가 부정확할 경우 심각한 결과를 초래할 수 있는지 또는 상식적으로 실수가 있을 수 있는지의 여부를 중복해서 확인해야 한다.

⇒ 사례

페업 절차를 밟고 있는 회사가 직원 중 한 명을 다른 회사에 추천하려고 한다. 두 회사의 고용주는 서로 잘 알고 지내는 사이였다. 이런 경우 일반적으로 추천을 받은 회사는 그 직원의 업무 경험에 대해 그대로 받아들여도 무방할 것이다. 그러나 새로운 업무에 대해 특정한 기술이나 자격이 필요한 경우 추천을 받은 회사는 해당 내용을 적절히 점검해야 한다.

- 개인정보의 정확성을 확보하기 위해 모든 합리적인 조치를 취했다라고 나중에 잘못되거나 오해를 야기할 수 있는 새로운 개인정보를 얻게 된다면, 해당 개인정보가 정확한 것인지 여부를 검토한 다음 가능한 빨리 그 개인정보를 삭제 또는 업데이트하거나 정정하는 조치를 취해야 한다.

1.4.7 정보주체의 이의제기에 대한 조치

- 개인정보의 정확성에 대하여 정보주체의 이의제기가 있는 경우 해당 개인정보가 정확한지 여부를 확인한 다음 정확하지 않으면 삭제하거나 정정해야 한다.
- 정보주체는 잘못된 개인정보의 정정을 요구할 수 있는 절대적 권리가 있다. 그러나 개인정보가 부정확하다고 해서 항상 삭제를 요구할 권리가 있는 것은 아니다.
- 정확성 원칙은 부정확한 개인정보를 지체 없이 삭제하거나 정정하기 위해 모든 합리적인 조치를 취할 것을 요구하고 있다. 경우에 따라서는 개인정보를 삭제하는 것이 더 합리적일 수도 있다. 따라서 정보주체가 부정확한 개인정보를 삭제해 달라고 요구해 온 경우 그 요청을 진지하게 검토하는 것이 바람직하다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제5조(개인정보 처리 원칙)제1항(d) ■ 제16조(정정권) ■ 제17조(삭제권) ■ Guidelines on transparency under regulations 2016/679, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제36조(개인정보의 정정·삭제)

1.5 보유기간 제한의 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 어떤 정보를, 어떤 목적으로 보유하는지 알고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보유기간을 정당화할 수 있는 근거를 가지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 보유기간에 관한 정책을 문서화 하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보를 정기적으로 검토하여 목적 달성 시 삭제 등의 조치를 하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체의 삭제권을 준수하기 위한 적절한 절차를 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.5.1 보유기간 제한 원칙이란?

- ‘보유기간 제한(storage limitation)’ 원칙이란 필요한 기간 이상 개인정보를 보유해서는 안 된다는 원칙이다. 개인정보를 공정하고 합법적으로 수집해서 이용한다고 하더라도 실제 필요한 기간보다 오래 보유할 수는 없다.
- GDPR은 개인정보의 보유기간에 대해서 구체적인 기간이나 기준을 설정해 두고 있지는 않다. 보유기간은 전적으로 특정 목적을 위해 해당 개인정보가 얼마나 오래 필요하지에 달려 있다.
보유기간 제한 원칙은 개인정보 최소처리 원칙 및 정확성 원칙과 매우 밀접한 관계가 있다.

1.5.2 보유기간 제한의 중요성

- 개인정보가 더 이상 필요하지 않을 때 삭제하거나 익명화하면 처리 목적과 무관하거나 과도하거나 부정확한 개인정보의 처리를 막을 수 있게 되어 개인정보 최소처리 원칙 및 정확성 원칙을 준수하는 데 도움이 되고 개인정보를 잘못 이용할 위험도 줄여 준다.
- 법적 관점에서 볼 때 개인정보를 오랫동안 보유하는 것은 불필요하며 그렇게 해야 할 합법적인 근거를 찾기도 어렵다. 실무적인 관점에서 보더라도 개인정보를 필요 이상으로 오랫동안 보유하는 것은 비효율적이며 보유 및 보안에 불필요한 비용을 지출하게 한다.

- 컨트롤러는 정보주체의 접근권 요청에 대응해야 하는데 필요 이상으로 개인정보를 오랫동안 보유하고 있을 경우 이에 대한 대응도 쉽지 않다. 이 경우 보유기간 및 삭제에 대한 명확한 정책을 공개하면 정보주체의 접근권이나 삭제권 요청에 따른 부담도 줄일 수 있다.

1.5.3 보유기간의 문서화

- 개인정보 보유 정책 또는 일정표에는 보유 중인 개인정보의 유형, 이용 목적, 보유 기간 등이 포함되어 있다. 개인정보 보유 정책은 여러 유형의 개인정보에 대한 표준적인 보유기간을 설정하고 문서화하는데 도움이 된다.

개인정보 보유 정책 또는 일정표는 정보자산관리대장의 일부를 구성할 수도 있고 개인정보 처리에 관한 일반적인 문서의 일부를 구성할 수도 있다. 기록 관리 규정에 따라 가능하면 개인정보의 유형마다 표준적인 보유기간을 설정해서 문서화해야 한다.

- 조직이 실제로 보유기간을 준수하고 있는지 여부를 확인하고 적절한 간격으로 보유 상태를 점검하기 위한 시스템을 갖추는 것이 바람직하다. 또한 필요한 경우 조기 삭제를 허용할 수 있도록 정책에 충분한 유연성을 두어야 한다. 예를 들어, 실제로 개인정보를 이용하고 있지 않다면 그 개인정보를 계속 보유할지 여부를 검토해야 한다. 다만, 개인정보를 간헐적으로 이용하여 개인정보 처리에 따른 위험이 작은 소규모 기업이라면 문서화된 개인정보 보유 정책을 수립하지 않을 수 있다. 그러나 이 경우에도 보유하고 있는 개인정보를 정기적으로 점검하고 더 이상 필요하지 않은 개인정보는 삭제하거나 익명화해야 한다.

⇒ 사례

국가기록원은 기록의 보존과 파기를 포함하여 공공기관을 위한 실무지침을 제시하고 있어 개인정보 보유기간 제한 원칙을 준수하는데 도움이 되고 있다.

1.5.4 보유기간의 설정 방법

- GDPR은 개인정보의 보유기간에 대해서 구체적인 기간이나 기준을 설정해 두고 있지 않다. 따라서 개인정보의 처리 목적을 고려해서 컨트롤러가 스스로 보유기간을 정해야 한다. 보유기간이 어느 정도 필요한지에 대해서 판단할 수 있는 최적의 위치에 있는 사람은 컨트롤러 자신이기 때문이다.

- 컨트롤러는 개인정보를 식별 가능한 상태로 보유해야 하는 정당한 이유도 설명할 수 있어야 한다. 개인을 식별할 필요가 없다면 더 이상 식별이 불가능하도록 개인정보를 익명화해야 한다.

명시한 목적을 위해 여전히 해당 개인정보의 처리가 필요하다면 그 목적 달성 시까지 보유가 가능하나, 단지 만약의 경우를 대비하거나 이용 가능성이 아주 적은 경우까지 고려하여 개인정보를 보유해서는 안 된다.

⇒ 사례

은행은 고객의 이름, 주소, 전화번호, 생년월일 등 많은 개인정보를 보유하고 있으며 해당 정보를 보안절차의 일부로 이용하기도 한다. 고객이 은행에 계좌를 가지고 있는 한 은행이 이들 정보를 보관하는 것은 적절하다. 또한 계좌가 폐쇄된 후에도 은행은 일정 기간 동안 법적 또는 운영상의 이유로 일부 개인정보는 계속 보관해야 할 수 있다.

⇒ 사례

은행은 사기 방지를 위해 ATM기기에 설치된 CCTV 시스템의 개인영상정보를 몇 주 동안 보유해야 할 필요가 있다. 피해자가 은행계좌를 확인할 때까지는 수상한 거래가 드러나지 않을 수 있기 때문이다. 상대적으로 음식점에서 발생한 사건은 매우 빨리 확인되므로 CCTV 시스템의 개인영상정보를 짧은 시간 동안만 보유하면 된다. 다만, 음식점은 범죄 사실이 경찰에 알려진 경우에는 경찰이 해당 개인영상정보를 수집해 갈 때까지 보유해야 한다.

⇒ 사례

채권추심회사는 채권자를 대신해서 채무자를 찾기 위해서 채무자에 관한 개인정보를 보관할 수 있다. 그러나 일단 채무자를 찾아서 채권자에게 보고하고 나면 채무자에 관한 정보는 더 이상 보유할 필요가 없다. 채권추심회사는 채무자의 개인정보를 보유할 충분한 이유가 없는 한 해당 정보를 시스템에서 삭제해야 한다.

- 거래관계가 종료되더라도 당장 모든 개인정보를 삭제해야 할 필요가 없을 수 있다. 관계가 종료되면 그 정보주체와의 관계에 관한 기록을 남겨 두어야 할 필요가 있을 수 있기 때문이다. 예컨대 그 정보주체와 관계가 존재했던 사실과 그 관계가 끝났음을 확인할 수 있도록 정보의 일부를 보유해야 할 필요가 있을 수도 있다.

⇒ 사례

사업자는 고객이 제기할 수 있는 미래의 불만을 처리하기 위하여 이전 고객에 관한 개인정보의 일부를 보유할 수 있다.

⇒ 사례

사업자는 근로자가 퇴사할 때 그 근로자와 관련해서 보유하고 있는 개인정보를 검토해야 한다. 예를 들어, 연금 제공에 필요한 개인정보는 보유해야 하지만, 직원의 비상연락처, 과거 주소 등 다시는 필요가 없을 것 같은 개인정보는 기록에서 삭제해야 한다.

⇒ 사례

사업자는 이전 고객으로부터 직접 마케팅을 위해 이용하고 있는 개인정보의 처리 정지를 요구받으면, 향후 직접 마케팅 활동에 해당 고객을 포함하지 않도록 하여야 한다.

- 향후 발생할 수도 있는 법적 청구를 방어하기 위해 개인정보를 보유해야 할 필요가 있는 경우도 있다. 그러나 이 경우에도 법적 청구와 관련이 없는 정보는 삭제해야 한다. 또한, 다른 이유가 존재하지 않는 한 더 이상 법적 청구를 주장할 수 없게 된 경우에는 해당 정보를 모두 삭제해야 한다.

⇒ 사례

고용주는 명확한 업무상의 이유가 존재하지 아니하는 한 근로자 채용 과정에서 발생할 수 있는 분쟁과 관련한 소 제기 기간이 지나면 더 이상 미채용자에 관한 채용기록을 보유해서는 안 된다.

- 법령상 요구나 의무 준수를 위한 개인정보의 보유는 필요한 개인정보의 보유로 볼 수 있다. 예컨대, 납세, 감사 등의 목적에 필요한 정보나 건강, 안전 등과 관련된 정보는 법령상 보유이 요구되거나 허락되는 경우가 많다. 이와 같은 요건을 준수하기 위해 개인정보를 보유할 경우 필요 이상 보유한 것으로 간주되지 않는다.
- 관련 업계의 표준이나 가이드라인도 고려해야 한다. 예를 들어, 신용정보회사가 업계 가이드라인에 따라 신용정보를 10년간 보유하는데 소비자의 동의를 받았다고 하자. 이와 같은 업계 가이드라인은 표준 보유기간을 위한 좋은 예가 된다. 그러나 업계 표준이 보유기간의 정당성을 보장하지는 않는다. 컨트롤러는 보유기간의 정당성을 설명할 수 있어야 하고 계속해서 보유기간의 정당성을 검토해야 한다.

마지막으로, 컨트롤러는 해당 개인정보를 보유해야 할 필요성과 그 개인정보의 보유가 정보주체의 프라이버시에 미칠 영향을 비교 분석해야 하고, 개인정보의 보유가 항상 공정하고 적법하도록 노력해야 한다.

1.5.5 보유기간의 재검토

- 컨트롤러는 표준 보유기간이 지난 후에도 여전히 개인정보를 보유할 필요가 있는지 여부를 검토하고 더 오래 보유해야 할 이유가 명확하지 않으면 삭제하거나 익명화해야 한다. 자동화 시스템을 통해서 사전에 정해진 기간이 지나면 자동적으로 정보를 삭제할 수 있다.

표준 보유기간이 길거나 정보주체에게 상당한 영향을 미칠 가능성이 있는 경우에는 정기적으로 개인정보의 보유 실태를 점검하는 것이 바람직하다. 또한, 개인정보에 대해 정해진 보유기간이 없는 경우에도 여전히 해당 개인정보가 필요한지 여부를 정기적으로 검토해야 한다.

- 그러나 얼마나 자주 규칙적으로 검토를 해야 하는지에 대한 명확한 기준이나 규칙은 없다. 정보주체에 대한 프라이버시 위험과 함께 컨트롤러가 활용할 수 있는 자원을 고려해서 실행하되, 컨트롤러는 개인정보 보유 필요성 및 검토 주기를 정당화할 수 있어야 한다.

정보주체는 ‘더 이상 특정 목적을 위해 필요하지 않은 개인정보’의 삭제를 요구할 수 있는 절대적 권리가 있다. 이 경우 컨트롤러는 정보주체의 삭제 요구에도 불구하고 여전히 개인정보를 보유할 필요가 있는지 여부를 검토해야 한다.

1.5.6 개인정보의 파기 방법

- 개인정보는 삭제 외에 익명화도 가능하다. 그러나 개인정보를 오프라인으로 전환해서 저장하는 것은 영구적으로 삭제하거나 익명화하는 것과는 차이가 있다. 개인정보를 오프라인으로 전환해서 저장하는 경우 오·남용 위험을 감소시킬 수는 있으나 여전히 개인정보를 처리하고 있는 것으로 간주된다.

따라서 개인정보의 보유를 정당화할 수 있는 경우에만 개인정보를 삭제하지 않고 오프라인으로 저장할 수 있다. 또한 오프라인으로 저장된 개인정보도 정보주체가 행사하는 접근권의 대상이 되며, 그밖에 모든 개인정보 처리 원칙과 권리 행사를 준수해야 한다.

- ‘삭제’라는 단어는 전자적 데이터와 관련해서는 다른 의미를 가질 수 있다. 전자적 데이터는 모든 흔적을 삭제하거나 지우는 것이 항상 가능한 것은 아니기 때문이다. 중요한 것은 데이터를 더 이상 사용할 수 없도록 하는 것이다. 개인정보를 삭제할 때에는 백업 정보도 함께 삭제해야 한다.

삭제에 대한 대안은 더 이상 ‘개인정보’를 식별할 수 없도록 익명화하는 것이다. 키 코드화와 같이 가명처리된 개인정보는 일반적으로 여전히 식별이 가능하므로 삭제로 볼 수 없다. 가명처리는 개인정보 최소화처리 원칙 및 안전성 조치 원칙과 같은 개인정보 처리 원칙을 준수하는 데는 유용한 도구가 될 수 있지만 보유 제한 원칙은 피할 수 없다.

1.5.7 연구목적 등을 위한 보유

- 개인정보를 ① 공공의 이익을 위한 보유 목적, ② 과학적·역사적 연구 목적, ③ 통계적 목적으로만 보유할 경우 그 기간을 연장할 수 있다.

일반적으로 ‘만일에 대비해서’ 향후 유용할지 모른다는 이유로 무한정 오랫동안 개인정보를 보유할 수는 없지만, 공익 목적 보유, 연구·통계 목적 보유의 경우에는 예외가 인정된다. 다만, 정보주체를 보호하기 위한 적절한 안전장치를 갖춰야 한다. 예를 들어, 어떤 경우에는 가명처리가 적절할 수 있다.

- 공익 목적 및 연구·통계 목적으로 보유한 개인정보는 나중에 다른 목적으로 이용할 수 없다. 특히 특정 개인에게 영향을 미치는 의사결정에 이용할 수 없다. 또한, 다른 컨트롤러가 공익 목적 및 연구·통계 목적으로 해당 개인정보에 접근하는 것을 방해하지는 않지만, 그들도 개인정보를 수집·이용할 때 목적 외 이용 금지 원칙을 준수하여야 한다.

1.5.8 공유 개인정보의 삭제 등

- 개인정보를 더 이상 공유할 필요가 없게 되었을 때 발생할 수 있는 일에 대해 미리 당사자 사이에 합의가 있어야 한다. 어떤 경우에는 공유 정보를 제공자에게 모두 반환하는 것이 좋으나, 다른 경우에는 모든 공유 정보를 삭제하는 것이 좋을 수 있다.

⇒ 사례

A사와 합병을 준비 중인 B사는 A사의 고객 개인정보를 공유하는 경우가 있게 되는데, 이 경우 B사는 해당 정보를 합병 준비 목적으로만 비밀로 이용하기로 되어 있다. 이 경우 합병이 결정되었다면 B사는 사본을 보관하지 않고 고객 개인정보를 A사에 반환하여야 한다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제5조(개인정보 처리 원칙)제1항(e) ■ 제17조(삭제권) ■ 제30조(처리활동의 기록)제1항(f) ■ 제89조(공적기록, 과학·역사연구, 통계목적 처리를 위한 안전조치)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제15조(개인정보의 수집·이용)제2항 ■ 제17조(개인정보의 제공)제2항 ■ 제18조(개인정보의 목적외 이용·제공 제한) ■ 제21조(개인정보의 파기) ■ 제36조(개인정보의 정정·삭제)

1.6 무결성·기밀성의 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보 처리 관련 위험을 분석하고 보안 수준 평가에 활용하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보안조치를 결정할 때 최신 기술, 이행 비용 등을 고려하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보안정책을 가지고 있고 이행하기 위한 조치를 취하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보안 정책과 수단을 정기적으로 검토하고 개선하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 상황에 따라 암호화 또는 가명처리 조치를 하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 문제가 발생한 경우 백업을 통해 개인정보의 복원을 보장하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보안조치의 효과성을 정기적으로 점검테스트하고 개선 조치를 취하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.6.1 무결성·기밀성 원칙이란?

- ‘무결성·기밀성(integrity and confidentiality)’ 원칙이란 보유하고 있는 개인정보를 안전하게 보호하기 위해 적절한 보안조치를 취해야 한다는 원칙이다. 따라서 무결성·기밀성 원칙은 ‘보안성 원칙(security principle)’이라고도 부른다.

컨트롤러는 적절한 기술적·관리적 조치를 통하여 권한 없는 처리, 불법적 처리, 우발적 손·망실, 파괴 또는 훼손 등을 막을 수 있다.

- 이와 같은 기술적·관리적 조치에는 위험분석, 프로세서에 대한 관리·감독, 가명화 또는 익명화, 기밀성·무결성 및 가용성의 보장, 보호조치의 효과를 검증하고 개선작업을 수행하기 위한 적절한 절차 등이 포함된다.

여기서 말하는 정보보안에는 전자적 공격으로부터 네트워크 및 정보시스템을 보호하는 것만을 의미하는 것이 아니라 물리적 보안과 관리적 대책도 포함된다.

GDPR 제32조(처리의 보안)는 보안성 원칙과 밀접한 관계가 있다. 제32조 제1항은 최신기술, 이행 비용, 처리의 성격·범위·상황·목적, 정보주체의 권리와 자유에 미치는 위험의 심각성 등을 고려하여 적절한 보안 수준을 보장하기 위한 기술적·관리적 조치를 이행하도록 요구하고 있다.

1.6.2 무결성·기밀성 원칙의 내용

- ‘보안성 원칙’에 관한 보다 세부적인 설명은 GDPR 제32조의 기술적·관리적 보호조치에 대해서 기술하고 있는 ‘제4장. 기업의 책임성 강화’에 관한 부분을 참조할 수 있다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제5조(개인정보 처리 원칙)제1항(f)■ 제28조(프로세서의 책임)■ 제32조(처리의 보안)■ 전문 제39항, 제81항, 제83항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제3조(개인정보보호 원칙)■ 제21조(개인정보의 파기)■ 제36조(개인정보의 정정·삭제)■ 제29조(안전조치의무)

1.7 책임성의 원칙



셀프 체크리스트

Self Check List

	예	아니오
• 최고경영자 및 조직 전체 차원에서 GDPR 준수에 대한 책임을 지고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• GDPR 준수를 위해 취한 조치의 증거를 보관하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• GDPR이 요구한 기술적·관리적 조치를 이행하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 적절한 간격으로 관련 조치들을 검토하고 업데이트 하는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.7.1 책임성 원칙이란?

- ‘책임성(accountability)’ 원칙이란 GDPR의 준수에 대해서 책임을 지고 그 준수를 입증할 수 있어야 한다는 원칙이다. 준수 여부를 입증할 수 있으려면 적절한 기술적·관리적 조치와 그에 관한 기록이 있어야 한다.

적절한 기술적·관리적 조치에는 개인정보처리방침의 채택 및 시행, privacy by design and by default, 개인정보 위탁처리에 대한 서면 계약, 개인정보 처리 활동에 관한 문서의 유지, 적절한 보안 조치의 이행, 개인정보 침해사고의 기록 및 고지, 개인정보 영향평가의 시행, DPO 임명, 행동규약 준수 및 개인정보 보호 인증 취득 등이 포함될 수 있다.

- 이와 같이 책임성 원칙은 개인정보보호를 위한 일상적인 관행을 의미하므로 컨트롤러는 시행한 조치들을 지속적으로 검토하고 업데이트해야 한다.

컨트롤러가 개인정보관리체계를 도입할 경우 이와 같은 책임 조치를 구체화하고 조직 전체에 개인정보보호 문화를 조성하는 데 도움이 된다.

책임성 원칙은 정보주체의 신뢰확보, 기업의 경쟁력 강화 등을 위해서 중요하지만, 책임성 원칙을 준수하지 못하면 과징금 등에서도 손해를 볼 수 있다.

1.7.2 책임성 원칙의 내용

- 책임성 원칙의 준수는 단지 점검표를 체크하는 것만으로는 달성하기 어렵다. 개인정보 보호를 위한 접근 방식 자체가 사전 예방적이고, 조직화되어 있어야 하며, 해당 조치들을 입증할 수 있어야 한다.
 - GDPR은 컨트롤러가 책임을 준수하기 위해 해야 할 모든 사항을 명시하고 있지는 않다. 다만, 앞에서 설명한 바와 같이 책임 준수에 필요한 몇 가지 조치들을 규정하고 있다. GDPR 제24조제2항은 GDPR 준수를 보장하고 입증할 수 있는 기술적·관리적 조치를 시행하고, 리스크에 기반을 둔 비례적인 대책을 마련해야 하며, 필요에 따라 조치를 검토하고 업데이트해야 한다고만 규정하고 있다.
- 이들 조치 중 일부는 의무적인 것이고 일부는 자발적인 것이다. 어떤 개인정보를 보유하고 있고 어떤 목적으로 이용하느냐에 따라 달라진다. 또한 컨트롤러의 규모에 따라서 책임성 원칙을 달성하기 위한 방법도 달라질 수 있다.
- 규모가 큰 조직이라면 조직 전체에 체계적이고 입증 가능한 규정 준수 문화를 정착시키기 위해 개인정보보호 관리체계를 도입하는 것이 바람직하다. 이 경우 개인정보보호 관리체계에는 적어도 아래 사항이 포함되어야 한다.
 - GDPR이 요구하는 프로그램의 견고한 통제(robust program controls)
 - 적절한 보고 체계
 - 평가 절차
 - 규모가 작은 조직이라면 좀 더 적은 규모의 접근 방법을 채택할 수 있다. 그러나 이 경우에도 최소한 아래의 사항은 포함되어야 한다.
 - 개인정보보호에 대한 임직원의 충분한 이해와 인식의 확보
 - 개인정보 처리를 위한 포괄적이고 비례적인 정책 및 절차의 시행
 - GDPR 준수를 위해 수행한 업무의 내용 및 그 이유의 기록과 보유
- ‘책임성 원칙’에 관한 보다 세부적인 설명은 ‘제4장. 기업의 책임성 강화’에 관한 부분을 참조할 수 있다.

<p>GDPR 관련 규정</p>	<ul style="list-style-type: none"> ■ 제5조(개인정보 처리 원칙) 제2항 ■ 제12조~제14조(정보주체의 알권리) ■ 제24조(컨트롤러의 책임) ■ 제25조(privacy by design and by default) ■ 제28조(프로세서의 책임) ■ 제30조(처리활동의 기록) ■ 제32조(처리의 보안) ■ 제33조(개인정보 침해 신고) 및 제34조(개인정보 침해 통지) ■ 제35조(개인정보 영향평가) 및 제36조(사전협의) ■ 제37조~제39조(DPO 지정, 지위 및 직무) ■ 제40조~제43조(행동규약, 정보보호인증 등) ■ 전문 제39항, 제42항, 제58항~제61항, 제71항, 제74항, 제78항, 제81항, 제82항, 제83항, 제84항, 제85항~제95항, 제97항~제98항, 제100항
<p>한국 개인정보보호법 관련 규정</p>	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제28조(개인정보취급자에 대한 감독) ■ 제29조(안전조치의무) ■ 제31조(개인정보보호책임자의 지정) ■ 제32조의2(개인정보 보호 인증) ■ 제33조(개인정보 영향평가) ■ 제34조(개인정보 유출 통지 등)



처리의 합법성



Point

- 개인정보의 합법적 처리를 위한 근거 또는 요건을 이해할 수 있다.
- 합법처리의 요건이 GDPR에서 수행하는 기능역할을 이해할 수 있다.

개인정보의 합법처리 근거

동의	정보주체의 동의에 기반하여 개인정보 처리 필요
계약	정보주체가 당사자인 계약의 이행을 위한 경우이거나 계약 체결 전에 정보주체의 요청으로 조치를 취하기 위하여 개인정보의 처리 필요
법적 의무	컨트롤러가 준수하여야 하는 법적 의무의 이행을 위하여 처리 필요
중대한 이익	정보주체 또는 다른 자연인의 중대한 이익(생명)을 보호하기 위하여 처리 필요
공적 업무 수행	컨트롤러에 부여된 공적 권한의 실행 또는 공익으로 실행되는 업무의 이행을 위하여 처리 필요
적법한 이익	컨트롤러 또는 제3자에 의하여 추구되는 적법한 이익을 위하여 처리 필요. 다만, 개인정보의 보호를 요하는 정보주체(특히 아동)의 기본적 권리와 자유나 이익이 우선하는 경우를 제외

2.1 합법처리의 근거



셀프 체크리스트

Self Check List

	예	아니오
• 각각의 목적마다 가장 적합한 법적 근거를 제시하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 목적 달성을 위한 다른 합리적인 방법은 없는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 목적별로 합법처리의 근거를 문서화 하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 고지사항에 처리 목적과 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 민감정보 또는 범죄정보에 특유한 처리 조건을 파악해 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.1.1 합법처리의 근거란?

- 합법처리의 근거(lawful basis for processing)란 개인정보의 처리를 정당화 해주는 법적 근거를 말한다. GDPR 제6조제1항은 개인정보를 합법적으로 처리할 수 있는 6가지 요건을 규정하고 있다. 다만, 공공기관이 공무 수행을 위하여 처리한 경우 '적법한 이익'을 합법처리의 근거로 제시할 수 없다.

- ① (동의) 정보주체가 특정 목적을 위해 개인정보 처리에 명확히 동의한 경우
- ② (계약) 정보주체가 당사자인 계약의 이행 또는 계약 체결 전 정보주체의 요청에 응하기 위하여 필요한 경우
- ③ (법적 의무) 컨트롤러에게 적용되는 법령상 의무(계약상 의무 제외) 준수를 위하여 필요한 경우
- ④ (중대한 이익) 정보주체 또는 제3자의 중대한 이익(생명)을 보호하기 위하여 처리가 필요한 경우
- ⑤ (공적 업무 수행) 공무 수행 또는 공적 권한 행사를 위하여 필요하고 그 업무와 권한이 법령상 명확한 근거를 가지고 있는 경우
- ⑥ (적법한 이익) 컨트롤러 또는 제3자의 적법한 이익 추구 목적을 위하여 필요한 경우
 - 다만, 정보주체(특히 아동)의 이익, 기본적 권리 및 자유가 그 이익보다 중요한 경우는 제외

- EU 회원국은 GDPR 제6조제2항에 따라 법적 의무 준수(제6조제1항(c)) 또는 공무 수행(제6조제1항(e))을 위한 개인정보 처리의 합법 요건에 관한 특칙을 규정할 수 있으므로 이에 대해서는 회원국의 법률을 검토할 필요가 있다.
합법처리의 근거 중 하나가 다른 것들보다 더 낮거나 더 중요한 것은 아니다. 어떤 근거가 가장 활용하기에 적합한지는 정보주체와의 관계 및 개인정보 처리의 목적에 달려 있다.
- 합법처리의 근거는 정당한 이유 없이 나중에 다른 근거로 바꿀 수 없으므로 처음부터 신중하게 검토되어야 한다. 특히 동의를 합법처리의 근거로 한 경우 다른 근거로 변경할 수 없다.
- 다만, 목적이 변경되었더라도 새로운 목적이 최초 목적과 양립 가능한 경우(제6조4항)(원래 합법처리의 근거가 동의 혹은 제23조1항인 경우 제외)에는 최초의 합법처리 근거에 따라 처리를 계속할 수 있다.

2.1.2 ‘필요한(Necessary)’ 경우의 의미

- 동의를 제외하고 합법처리의 요건은 ‘필요한’ 경우에 의존한다. 여기서 필요하다는 것은 개인정보 처리가 ‘절대적으로’ 필수적이어야 한다는 것을 의미하지는 않는다. 하지만 개인정보 처리가 단지 유용한 것 이상으로 필요하여야 하고, 일반적인 관행(standard practice) 이상으로 필요하여야 한다. 또한 특정한 목적을 달성하기 위한 것이어야 하고 비례적이어야 한다.
- 개인정보를 처리하지 않거나, 덜 처리하며 덜 침해하는 다른 방법으로도 합리적으로 목적을 달성할 수 있다면 합법적 처리로 인정받지 못한다.
또한 특정한 방법으로 사업을 운영하기로 선택했기 때문에 해당 개인정보의 처리가 필요하다고 주장하는 것으로는 충분하지 않다. 문제는 그 처리가 명시된 목적을 위해 객관적으로 필요한 것인지 여부 및 선택한 방법 중에서 필수적인 부분인지 여부에 달려 있다.

2.1.3 합법처리 근거의 중요성

- GDPR은 개인정보를 ① 합법적이며, ② 공정하고, ③ 투명하게 처리할 것을 요구한다(개인정보 처리 제1원칙). 개인정보 처리가 합법처리의 요건을 갖추지 못한 경우 그 처리는 불법적인 처리가 되고 제1원칙을 위반한 것이 된다. 또한 정보주체는 불법적으로 처리된 개인정보의 삭제를 요구할 권리가 있다.

- GDPR 제13조 및 제14조에 따라 정보주체가 고지 또는 통지받을 수 있는 권리에는 합법처리의 근거에 관한 정보도 포함된다. 따라서 개인정보를 처리하기 전에 정보주체에게 합법처리의 근거를 명시해야 한다.
- 합법처리의 근거는 정보주체의 권리행사에도 영향을 미친다. 다시 말해 합법처리의 근거에 따라 정보주체의 권리행사가 제한을 받게 되는 경우가 있다.
예를 들어, 정보주체는 합법처리의 근거가 무엇이든 직접 마케팅 목적을 위한 개인정보 처리에 대해서는 언제든지 반대할 절대적 권리를 가진다. 그러나 나머지 권리들은 항상 절대적인 것은 아니다.
자동화된 의사 결정, 프로파일링 등의 반대권은 합법처리의 근거에 따라 영향을 받게 되므로 정보주체의 반대권 행사를 방어하고 싶다면 정보주체에 대한 고지사항에 합법처리의 근거를 보다 상세히 알려야 한다.

2.1.4 합법처리 근거의 선택

- 어떤 합법처리에 근거해서 개인정보를 처리할지를 결정하는 것은 전적으로 처리의 목적과 환경에 따라 달려 있다. 따라서 개인정보를 처리하려는 이유를 생각해 보고 상황에 가장 적합한 근거를 선택해야 한다.
합법처리의 근거가 두 개 이상인 경우에는 처음부터 모든 근거를 식별하고 문서화해 두어야 한다. 합법처리의 근거에는 순서가 없으므로 어떤 근거가 더 좋고, 더 안전하고, 더 중요한 것인지에 대해서 구분이 없다.
- 일반적으로 법적 의무 준수, 정보주체와 계약 체결, 중대한 이익 보호, 공무 수행 등을 위한 개인정보 처리는 그 목적이 비교적 명확하므로 합법처리의 근거도 선택하기 쉽다. 그러나 적법한 이익 또는 동의 중 하나를 합법처리의 근거로 선택할 때에는 아래와 같은 상황을 광범위하게 고려해야 한다.
 - 처리가 누구의 이익을 위한 것인가?
 - 정보주체가 그와 같은 처리를 예상할 수 있는가?
 - 정보주체와 어떤 관계인가?
 - 정보주체에 비하여 우월적인 지위에 있지 않은가?
 - 처리가 정보주체에게 어떤 영향을 미치는가?
 - 정보주체가 신체적 또는 정신적으로 취약한 입장에 있는가?
 - 정보주체 중 일부가 처리에 반대할 가능성이 있는가?
 - 정보주체의 요구 시 언제든지 처리를 중단할 수 있는가?

- 만약 개인정보를 계속적으로 처리해야 할 필요가 있고, 그와 같은 처리가 사람들의 합리적인 기대와 일치하고, 정보주체에게 어떤 부당한 영향도 미치지 않을 것이라는 사실을 입증할 수 있다면 ‘적법한 이익’을 합법처리 근거로 선택할 수 있다.
반면에 개인정보에 대한 모든 통제권과 책임(동의 철회, 처리 제한 등)을 정보주체에게 부여하고 싶다면 정보주체의 동의를 합법처리의 근거로 선택할 수 있다.

2.1.5 공공기관에 대한 특칙

- 합법처리의 근거는 공공기관에 대해서도 동일하게 적용된다. 공공기관도 처리 목적에 따라 합법처리의 근거를 선택할 수 있다.
공공기관이 법령상 규정된 공무를 수행하기 위하여 개인정보를 처리할 때에는 ‘공무 수행’을 합법처리의 근거로 선택할 수 있다. 그러나 ‘공무 수행’ 이외의 목적을 위한 처리라면 다른 합법처리의 근거를 고려해야 한다.
- 처리의 성격이 공무가 아니라면 공공기관이라도 정보주체의 동의나 적법한 이익을 합법처리의 근거로 선택할 수 있다. 공공기관은 동의나 적법한 이익을 합법처리의 근거로 채택하는데 일부 한계가 있지만 반드시 금지되는 것은 아니다.

⇒ 사례

대학은 공공기관으로 분류되기 때문에 교육·연구 목적으로 개인정보를 처리할 때에는 ‘공무 수행’을 합법처리의 근거로 선택할 수 있으나 동창회 관계 업무 수행 또는 학교 발전기금 모금 목적의 개인정보 처리는 ‘적법한 이익’과 ‘동의’를 고려하여야 한다.

2.1.6 합법처리 근거의 변경

- 합법처리의 근거는 개인정보를 처리하기 전에 결정해야 한다. 정보주체에게 합법처리의 근거를 고지한 후에 그 선택이 부적절했다는 것을 발견하더라도 합법처리의 근거를 변경하는 것은 어렵다.
처음부터 다른 합법처리의 근거를 적용할 수 있는 상황이었다 하더라도 합법처리의 근거를 소급해서 변경하는 것은 본질적으로 정보주체에게 불공평하고 책임성과 투명성 요건을 위반하는 결과를 초래할 수 있기 때문이다.

⇒ 사례

컨트롤러가 '동의'에 근거하여 개인정보를 처리하기로 결정하고 정보주체들의 동의를 얻었다. 이후 일부 정보주체들이 개인정보 처리에 대한 동의를 철회하자 컨트롤러는 합법처리의 근거를 '적법한 이익'으로 변경해서 동의 철회를 거부하고 계속해서 처리하고자 한다. 이 경우 원래 '적법한 이익'에 의존할 수 있었다더라도 컨트롤러는 이후 그와 같이 주장하거나 변경을 할 수 없다. 정보주체에게 선택권이 있다고 믿게 해놓고 나중에 선택권 행사를 거부하는 것은 본질적으로 정보주체에게 불공평하기 때문이다. 따라서 컨트롤러는 정보주체가 동의를 철회할 때 처리를 중단해야 한다.

- 따라서 처음부터 어떤 합법처리의 근거가 더 적절한지 사전에 철저히 평가하고 이를 문서화하는 것이 중요하다. 목적이 두 가지 이상인 경우, 개인정보 처리에 둘 이상의 합법처리 근거가 적용될 수도 있다. 그렇다면 처음부터 이 점을 분명히 해야 한다.
- 진정한 상황 변화가 있어서 합법처리의 근거를 변경해야 할 새롭고 예상치 못한 이유나 목적을 가지고 있다면 정보주체에게 그 사실을 알리고 변경을 문서화 하여야 한다.

2.1.7 추가 목적의 양립가능성 판단

- 시간에 따라 목적이 바뀌거나, 원래 예상하지 못했던 새로운 목적이 생기더라도 새로운 목적이 원래의 목적과 양립할 수 있다면 새로운 합법처리의 근거가 요구되지 않을 수 있다.
- 수집목적 외의 개인정보의 처리가 정보주체의 동의 또는 EU나 회원국의 법률에 근거하지 않은 경우에 컨트롤러는 그 다른 목적의 처리가 개인정보를 처음 수집한 목적과 양립가능성을 판단함에 있어서 GDPR 제6조제4항에 열거된 사항을 고려하여야 한다. 새로운 목적이 원래 목적과 양립 가능한 것인지 여부를 평가하기 위해 다음 사항을 모두 고려하여야 한다(제6조4항).
 - 최초 목적과 새로운 목적 사이의 연관성
 - 개인정보가 수집된 맥락 - 특히 정보주체와의 관계 및 정보주체가 합리적으로 예상 가능한 것인지 여부
 - 개인정보의 성격 - 예를 들어, 민감정보, 범죄정보 등
 - 새로운 처리가 정보주체에게 미칠 수 있는 결과
 - 적절한 안전장치가 있는지 여부 - 예를 들어, 암호화, 가명처리 등
- 하지만, 이와 같은 고려사항만으로는 충분하지 않고 새로운 목적이 가져올 전반적인 상황을 살펴야 한다. 새로운 목적이 원래 목적과 매우 다르거나, 예상치 못한 것이거

나, 개인에게 정당하지 않은 영향을 미치는 경우에는 일반적으로 양립성은 인정되지 않는다. 다만, GDPR은 아래와 같은 목적을 위한 개인정보의 추가 처리는 양립 가능한 합법적 처리로 보아야 한다고 규정한다(제89조).

- 공익에 대한 기록 목적
- 과학적 연구 목적
- 통계 목적

2.1.8 합법처리 근거의 문서화

- 책임성 원칙에 따라 컨트롤러는 GDPR을 준수하고 있다는 것을 입증할 수 있어야 하고 개인정보 처리를 위한 적절한 정책과 절차를 가지고 있어야 한다(제5조제2항). 이를 통해 컨트롤러는 합법처리의 근거를 적용하기 위해 적절한 노력을 기울였다는 것과 그 결정이 정당했다는 사실을 보여 줄 수 있다.
- 문서에는 처리 목적마다 어떤 근거에 의해서 처리하고 있고 그 같은 처리의 근거를 적용한 이유(정당성)를 기록해 두어야 한다. 그 기록이 합법처리의 근거를 입증하기에 충분하면 되고 기록을 위한 별도의 양식은 없다.

2.1.9 합법처리 근거의 고지

- 컨트롤러는 정보주체에 대한 고지사항에 처리별로 합법처리의 근거를 명시해야 한다.
GDPR의 투명성 원칙에 따라 정보주체에게 제공해야 할 정보는 아래와 같다(제13조 제1항(c), 제14조제1항(c)).
- 개인정보 처리의 목적
 - 합법처리의 근거

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제6조(처리의 합법성) ■ 제5조(개인정보 처리 원칙)제1항(b) ■ 제13조 및 제14조(정보를 제공받을 권리) ■ 제3장(정보주체의 권리) ■ 제24조(컨트롤러의 책임) ■ 전문 제39항, 제40항, 제50항, 제61항 ■ Guidelines on transparency under regulations 2016/679, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제3조(개인정보보호 원칙) ■ 제15조, 제17조, 제18조, 제23조, 제24조, 제24조의2, 제25조, 제26조

2.2 동의



셀프 체크리스트

Self Check List

	예	아니오
동의 방법		
• 동의가 가장 적합한 합법처리의 근거임을 확인하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 약관과 구분해서 별도로 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 이해하기 쉽고 간결하고 명확하고 평이한 언어로 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의를 서비스 제공의 전제조건으로 삼고 있지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 처리 목적·유형별로 구체적·개별적인 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
동의 기록		
• 동의 받은 날짜와 방법을 기록해 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에게 알린 내용을 기록해 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
동의 관리		
• 정기적으로 동의서를 검토해서 변경 사항을 체크·반영하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의 철회 방법을 공개하고 언제든지 쉽게 철회할 수 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의 철회에 대해 불이익을 주고 있지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.2.1 개요

- 컨트롤러는 개인정보 처리를 위한 다른 합법적인 근거를 찾기 어려운 경우 정보주체의 동의(consent)를 받아 개인정보를 처리할 수 있다. 그러나 일반적인 계약의 경우와 달리 개인정보 처리에 대한 동의는 적극적인 동의(positive opt-in)이어야 하고 정보주체에게 진정한 선택권이 부여되어야 하며 동의를 한 후에도 동의를 철회할 수 있는 철회권이 보장되어야 한다. 따라서 정보주체의 선택권 행사에 도움이 되도록 동의를 받기 전에 정보주체에게 개인정보의 처리 목적, 보유기간 등을 알기 쉽게 알려야 하고, 처리의 목적과 유형을 구체적으로 구분해서 개별적인 동의를 받아야 하며 모호하거나 포괄적으로 동의를 받아서는 안 된다.
- 동의는 자유로워야 하고 컨트롤러가 이를 입증할 수 있어야 한다. 정보주체에게 동의에 대한 선택권을 부여할 수 없다면, 동의를 서비스 제공의 전제조건으로 요구해서는 안 된다. 특히 고용관계에서는 동의에 의존해서 개인정보를 처리하는 것을 피해야 한다. 개인정보 처리에 대한 동의가 자신에게 미칠 영향을 알기 어려운 미성숙 아동에게 직접 서비스를 제공하거나 제품을 판매할 때에는 연령 확인 절차와 아동의 보호자 등의 동의 절차를 마련하여야 한다.
- 정보주체가 동의를 쉽게 철회할 수 있도록 언제든지 동의를 철회할 권리가 있다는 사실, 철회의 방법 등을 알기 쉽게 알려야 하고 정보주체가 동의를 철회한 경우에는 지체 없이 이에 따라야 하며 불이익을 주어서는 안 된다. 개인정보 처리 환경의 변화로 동의서가 현실과 맞지 않거나 차이가 나는 부분이 있는지 여부를 정기적으로 검토하여 동의서를 업데이트하는 것이 바람직하며 정보주체에게 적절한 간격으로 동의를 갱신할 수 있는 절차를 마련하는 것이 바람직하다.

2.2.2 동의의 유효요건 등

- 이 절에서 설명한 것 이외에 동의의 정의, 동의를 받는 방법, 동의의 유효 요건 등에 대하여 구체적인 설명은 ‘3. 동의’에 관한 부분을 참조할 수 있다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제4조(정의)제11항 ■ 제6조(처리의 합법성)제1항(a) ■ 제7조(동의의 조건) ■ 제9조(민감정보)제2항(a) ■ 제22조(프로파일링을 포함한 자동화된 의사결정) ■ 제49조(특정 상황에 대한 역외 이전 예외 조항) ■ 전문 제32항, 제38항, 제40항, 제42항, 제43항, 제171항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제4조(정보주체의 권리)제2호 ■ 제15조(개인정보의 수집·이용) ■ 제16조(개인정보의 수집제한) ■ 제17조(개인정보의 제공) ■ 제18조(개인정보의 목적 외 이용·제공제한) ■ 제19조(개인정보를 제공 받은 자의 이용·제공제한) ■ 제22조(동의를 받는 방법)

2.3 계약



셀프 체크리스트

Self Check List

	예	아니오
• 계약 체결 또는 이행을 위해 필요한 범위 내의 개인정보만 처리하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 계약을 합법처리의 근거로 삼은 것을 정당화 할 수 있는 이유를 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에 대한 고지사항에 계약 목적과 그 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.3.1 개요

- 컨트롤러는 계약(contract)을 개인정보 처리를 위한 합법처리의 근거로 주장할 수 있다. GDPR은 정보주체가 계약의 당사자가 되는 계약의 이행이나 계약 체결 전 정보주

체의 요청에 따른 절차(견적서 등)를 밟기 위해 필요한 경우 개인정보를 처리할 수 있다고 규정하고 있다(제6조제1항(b)).

2.3.2 계약이 합법처리의 근거로 인정되는 경우

- 컨트롤러는 아래와 같은 사유가 있는 경우 계약을 개인정보 처리의 합법적인 근거로 삼을 수 있다.
 - 정보주체와 체결한 계약이 존재하고 그 계약에 따른 컨트롤러의 의무를 준수하기 위해 정보주체의 개인정보를 처리해야 하는 경우(연락처 등)
 - 정보주체와 체결한 계약이 존재하고 그 계약에 따른 정보주체의 의무를 확보하기 위해 정보주체의 개인정보 처리가 필요한 경우(결제정보 등)
 - 계약 체결 전이나 계약 체결을 위해 정보주체가 요청한 절차를 이행하기 위하여 정보주체의 개인정보 처리가 필요한 경우(견적서 제공 등)에는 실제 계약 체결이 성사되지 않더라도 합법처리의 근거가 될 수 있다.

⇒ 사례

자동차 보험에 가입하기 위하여 소비자는 여러 보험회사에 견적을 요청할 수 있다. 이 경우 보험회사는 견적을 준비하기 위해 운전자의 연령, 직업, 자동차의 제조일, 배기량 등과 같은 정보를 처리할 수 있다.

- 계약 체결을 위해 정보주체의 개인정보를 처리할 필요가 있더라도 그 계약이 다른 사람과 체결하려는 계약이라면, 다시 말해 정보주체가 계약체결의 당사자가 아니라면 적법처리의 근거로 선택할 수 없다.

또한 표준계약조항에 따라 개인정보 처리가 허용되고 있더라도 컨트롤러가 자신의 사업 목적으로 정보주체의 개인정보를 수집하거나 재사용하는 경우에는 계약체결을 적법처리의 근거로 주장할 수 없다.

컨트롤러가 해당 계약과 관련이 없는 다른 의무를 이행하기 위해 또는 제3자의 요청에 의해 계약 체결 전 조치를 취하기 위해 개인정보 처리가 필요한 경우에도 계약체결을 합법처리의 근거로 적용할 수 없다.
- 계약법상 계약으로서의 요건을 충족한 합의가 존재하면 된다. 해당 계약이 공식적으로 서명이 포함된 문서에 의하거나 문서화되어야 할 필요는 없다.

즉, 여기서 말하는 계약은 넓은 의미로 어떤 조건이 제시되고 받아들여졌다는 것을 의

미하고, 계약 당사자가 둘 다 법적 구속력을 가지려고 의도한 것이며, 상호 교환적인 요소가 포함되어 있으면 된다(일반적으로 돈과 재화의 교환이지만 어떤 가치의 교환이라도 상관없다).

2.3.3 계약에 ‘필요한(Necessary)’ 경우의 의미

- ‘계약에 필요하다’의 의미는 계약을 이행하거나 계약 체결 전 사전 절차를 밟기 위해 개인정보 처리가 절대적으로 필수적이어야 한다거나 유일한 방법이어야 한다는 것을 의미하는 것은 아니다.

그러나 개인정보 처리가 단지 유용하다는 이유만으로 안 되고 일반적으로 우리가 필요하다고 말할 때 의미하는 것 이상의 필요성이 있어야 한다. 또한 표준계약조항의 일부로 필요성이 규정되어 있더라도 그것만으로는 필요성이 인정되지 않는다.

- 필요성은 계약에 따른 서비스의 제공 또는 정보주체의 요청에 따른 조치의 이행을 위해서 필수적이고 표적화되어 있으며 비례적인 것이어야 한다. 서비스의 제공 또는 요구조치의 이행을 위하여 개인정보 처리 이외에 다른 합리적인 방법이 있거나 개인정보를 덜 침해하는 방법이 있다면 계약을 합법처리의 근거로 적용할 수 없다.
- 컨트롤러가 자신의 사업 모델을 보다 일반적으로 유지하기 위해 또는 해당 계약에 따른 서비스 제공에 필요한 이상의 다른 사업 목적을 위해 계약조항에 필요성을 포함시켰다 하더라도 그것은 합법처리의 근거가 될 수 없다. 이런 경우에는 ‘적법한 이익’과 같은 다른 합법처리 근거를 적용하여야 한다.

⇒ 사례

정보주체가 온라인 구매를 할 때 컨트롤러는 주문 상품을 배달하기 위해 정보주체의 주소를 처리해야 한다. 이 경우 계약 이행을 위하여 개인정보 처리가 필요하므로 계약은 합법처리의 근거가 된다. 그러나 정보주체가 구매한 품목에 근거하여 정보주체의 관심과 선호도를 프로파일링 하는 것은 계약 이행에 필요하지 않으므로 컨트롤러는 계약을 합법처리의 근거로 주장할 수 없다.

- 맞춤형 광고가 고객과의 관계 유지를 위한 유용한 방법이고 비즈니스 모델의 필수적인 부분이라고 하더라도 계약 이행을 위해 필요한 것이라고 볼 수는 없다. 그렇다고 계약에 필요하지 않은 개인정보 처리가 자동적으로 불법이라는 것을 의미하는 것은 아니다. ‘동의’, ‘적법한 이익’, ‘법적 의무’ 등 다른 합법처리의 근거를 찾으면 된다.

2.3.4 특수한 환경에서의 적용

2.3.4.1 서비스 개선

- 온라인 서비스 제공자는 흔히 서비스 개선을 위해 이용자들이 서비스를 어떻게 이용하는지에 대해 자세한 정보를 수집한다. 그러나 그와 같은 개인정보를 수집·이용하지 않고도 이용자에게 개선된 서비스를 제공할 수 있기 때문에 서비스 개선 목적을 위한 개인정보의 처리는 일반적으로 계약이행을 위해 필요한 것으로 간주되지 않는다. 이 경우 온라인 서비스 제공자는 동의 또는 적법한 이익과 같은 다른 합법처리의 근거를 찾아야 한다.
- 또한, 서비스의 개선 및 추가 가능성이 계약조건에 포함될 수 있지만, 그와 같은 처리는 일반적으로 이용자와 체결한 계약 이행에 객관적으로 필요한 것으로 간주되지 않는다. 따라서 컨트롤러는 기존 서비스를 개선하거나 서비스의 새로운 기능을 개발할 목적으로 개인정보를 처리하는 경우 계약(제6조제1항(b))을 합법처리의 근거로 이용할 수 없다.

2.3.4.2 사기방지

- 컨트롤러는 사기 방지를 위하여 고객의 온라인 행태를 모니터링하거나 개인정보를 프로파일링 하는 경우가 있다. 이와 같은 목적의 개인정보 처리는 일정범위 내에서 정보주체와 체결한 계약이행에 필요한 것으로 볼 수도 있으나, 종종 객관적으로 필요한 것 이상으로 처리가 진행될 수도 있다. 이러한 경우에는 계약을 합법처리의 근거로 이용할 수 없다. 다만, 이 경우에도 개인정보 처리가 법적 의무 준수나 적법한 이익과 같은 다른 합법처리의 근거에 의존할 수 있다면 동의 없이 처리할 수 있다.

2.3.4.3 온라인 행태 광고

- 정보주체에 대한 추적과 프로파일링은 온라인 행태 광고와 같이 종종 온라인 서비스 제공을 위한 자금 조달 목적으로 행해지기도 한다. 하지만, 웹사이트 클릭 스트림과 구매 항목을 기반으로 하여 이용자의 취향과 라이프 스타일에 대한 프로파일링을 작성하는 행위는 계약 이행을 위해 필요한 것으로 인정되지 않는다. 프로파일링을 위해서 계약을 체결한 것이 아니라 특정 상품 및 서비스를 제공하기 위해서 계약을 체결한 것이기 때문이다.
- 일반적으로도, 온라인 행태 광고는 온라인 서비스의 필수 요소로 보고 있지 않는다. 즉, 온라인 행태 광고를 하지 못하면 서비스 제공 계약을 이행할 수 없다고 하는 논리

는 일반적으로 성립되지 않는 것이다. 이는 정보주체가 직접 마케팅 목적으로 개인정보를 처리하는데 반대할 권리를 인정하고 있는 제21조의 반대권이 절대적인 권리라는 점에서 자명하다.

- 이에 더하여, 온라인 행태 광고는 온라인 서비스 제공에 자금을 제공할 목적으로 이용되기 때문에 계약은 온라인 행태 광고에 대한 합법적인 근거를 제공할 수 없다. 그와 같은 목적의 개인정보 처리는 온라인 서비스의 제공을 지원할 수 있지만, 이용자와 서비스 제공자 간의 계약 목적과는 별개이므로 문제가 되는 계약의 이행에는 필요하지 않다.
- 또한, 컨트롤러는 유사한 특성을 가진 이용자들에게 맞춤형 타겟 광고를 하기 위해 해당 특성을 가진 개인을 식별하고자 이용자를 추적하거나 프로파일링을 수행하는 경우가 많다. 그러나 이용자에 대한 광고를 목적으로 이용자의 특성과 행태를 추적해서 다른 이용자와 비교하는 것은 객관적으로 보아 이용자와 체결한 계약을 이행하기 위해 필요한 것이라고 할 수 없으므로 계약에 근거하여 수행될 수 없다.
- 개인정보보호는 유럽인권조약(European Convention on Human Rights) 제8조에 의해서 보장되는 기본적 권리이고 GDPR의 주요 목적 중 하나는 정보주체에게 개인정보에 대한 통제권을 부여하는 것에 있으므로 개인정보를 거래 가능한 상품으로 볼 수는 없다는 것이 유럽 개인정보보호위원회(EDPB, European Data Protection Board)의 입장이다. 따라서 정보주체는 개인정보의 처리에 동의할 수는 있지만 기본적인 권리를 포기할 수는 없다. 또한 EDPB는 ePrivacy 입법의 요구, 행태광고에 대한 WP29의 의견¹¹, 쿠키 동의 가이드라인¹² 등에 따라 컨트롤러가 온라인 행태 광고에 필요한 개인정보를 처리하기 위해 쿠키를 사용하고자 할 때에는 정보주체의 사전 동의를 얻어야 한다고 설명하고 있다.¹³

2.3.4.4 콘텐츠의 개인화

- 특정 온라인 서비스의 경우 콘텐츠의 개인화는 필수적이거나 객관적으로 예상할 수 있으므로 이러한 경우 개인화를 위한 개인정보 처리는 이용자와 체결한 계약을 이행하기 위해 필요한 것으로 볼 수 있다. 콘텐츠의 개인화를 위한 개인정보 처리가 해당 온라인 서비스의 본질적인 것으로 볼 수 있을지 여부는 전적으로 제공되는 서비스의

11 제29조 작업반, Opinion 2/2010 on online behavioural advertising, 2010. 02.

12 제29조 작업반, Working Document 02/2013 providing guidance on obtaining consent for cookies, 2013. 02.

13 EDPS, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 2019. 04. 09., p.13.

기본 계약의 목적을 위해 콘텐츠 개인화가 객관적으로 필요하지 않은 경우, 예컨대 개인화된 콘텐츠가 본질적으로 서비스 이용에 필요한 것이 아니라 이용자의 참여를 높이기 위한 경우에는 계약에 근거하여 개인정보를 처리할 수 없고 다른 합법처리의 근거를 찾아야 한다.

이용자에게 뉴스 집계 서비스를 제공하는 온라인 뉴스 제공 사이트는 하나의 인터페이스를 이용하여 여러 온라인 소스들로부터 이용자가 관심을 가질 만한 콘텐츠를 찾아 맞춤형 콘텐츠를 제공하는 것을 본질적인 서비스로 한다. 이를 위해 뉴스 사이트는 이용자들에게 그들의 관심이 있는 콘텐츠를 선택할 수 있도록 콘텐츠를 분류하고, 분류된 콘텐츠를 웹 페이지에 표시하고, 웹 페이지를 로딩할 때 콘텐츠를 작성하도록 요구할 수 있다. 이 경우 뉴스 집계 서비스의 본질적 목적은 개인화된 콘텐츠의 제공에 있으므로 맞춤형 콘텐츠 제공을 위한 개인화는 온라인 뉴스 사이트와 이용자 간 체결된 계약의 이행을 위하여 객관적으로 필요한 것으로 간주될 수 있다. 따라서 계약을 합법적으로 근거로 활용할 수 있다.

많은 온라인 호텔 검색 엔진들이 이용자에게 특정한 지출 내역(프로파일)을 작성하기 위해 이용자의 과거 예약 내용을 모니터링하고 있다. 이 프로파일은 이후 이용자에게 검색 결과를 보여줄 때 특정 호텔을 추천하는 데 사용된다. 이 경우 이용자의 과거 행태 및 재무정보에 대한 프로파일링은 이용자와 체결한 계약의 이행 즉 이용자가 제공한 특정검색기준에 기반한 서비스의 제공을 위해 객관적으로 필요하지 않다. 따라서 계약을 합법처리의 근거로 활용할 수 없다.

이용자는 필요한 물건을 구입하기 위해 종종 온라인 마켓에서 구입할 물건을 검색해 본다. 이 때 온라인 마켓은 잠재 고객과 상호작용성을 높이기 위해 잠재 고객이 이전에 플랫폼에서 검색한 목록을 기반으로 하여 개인화된 제품을 제안하고 있다. 그러나 온라인 마켓의 이 같은 개인화 서비스는 온라인 판매 서비스 제공을 위하여 객관적으로 필요하지 않다. 따라서 계약을 합법처리의 근거로 활용할 수 없다.

2.3.5 계약을 합법처리의 근거로 할 때 주의할 사항

- 계약의 준비, 체결 및 이행을 위해 민감정보 또는 범죄정보가 필요한 경우 별도의 합법 처리 요건이 필요하므로 주의가 필요하다. 또한, 아등과 계약을 체결할 때에도 추가적인 합법처리의 요건이 적용되므로 유의해야 한다.

계약의 준비, 체결 및 이행을 위해 개인정보 처리가 필요하지 않다면 ‘동의’ ‘적법한 이익’ ‘법적 의무’ 등 다른 합법처리의 근거를 고려해야 한다.

- 계약을 합법처리의 근거로 할 경우 정보주체는 개인정보 처리 반대권과 자동 처리에 근거한 결정을 거부할 권리는 요구할 수 없다. 다만, 정보주체는 개인정보 이동권을 행사할 수 있다.

컨트롤러는 계약의 준비, 체결 및 이행을 위해 개인정보 처리가 필요하다고 결정한 내용을 문서화하고 정보주체에 대한 고지사항에도 처리의 목적과 합법처리의 근거를 포함해야 한다.

<p>GDPR 관련 규정</p>	<ul style="list-style-type: none"> ■ 제6조(처리의 합법성)제1항(b) ■ 전문 제44항 ■ Guidelines 2/2019 on the processing of personal data under Article 6(1), EDPB
<p>한국 개인정보보호법 관련 규정</p>	<ul style="list-style-type: none"> ■ 제15조(개인정보의 수집·이용)제1항제4호

2.4 법적 의무 준수



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보를 처리하기 전에 개인정보 처리가 필요한 법적 의무들을 파악·확인하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 법적 의무 준수를 위해 필요한 범위 내의 개인정보만 처리하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 법적 의무 준수를 합법처리의 근거로 삼은 것을 정당화 할 수 있는 이유를 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에 대한 고지사항에 법적 의무 준수 목적과 그 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.4.1 개요

- 컨트롤러는 법적 의무(legal obligation)를 준수하기 위하여 개인정보 처리가 필요한 경우 이를 합법처리의 근거로 할 수 있다. 이와 관련하여 GDPR은 컨트롤러에게 적용되는 법적 의무를 준수하기 위해서는 개인정보 처리가 필요하다고 규정하고 있다(제6조제1항(c)).
‘계약상 의무’는 법적 의무에 포함되지 않는다. 법령에 의해 컨트롤러에게 부과된 법적 의무를 준수·이행하기 위해 개인정보의 처리가 필요해야 한다. 따라서 합리적으로 개인정보를 처리하지 않고도 의무를 준수할 수 있다면 법적의무 준수를 합법처리의 근거로 적용할 수 없다.
- 컨트롤러는 법적 의무 준수를 합법처리의 근거로 결정한 내용을 문서화하고 그 같은 결정을 정당화할 수 있는지 확인해야 한다. 이를 위해 컨트롤러는 자신에게 의무를 부여하고 있는 법령의 조항을 구체적으로 파악하고 있어야 한다.

2.4.2 법적 의무의 의미

- ‘법적 의무’는 법령상 컨트롤러에게 부여된 의무만을 의미하고 계약에 따른 계약상의 의무는 이에 포함되지 않는다. 이 경우 법령은 EU법과 회원국법만을 의미하고 제3국의 법령은 포함되지 않는다(제6조제3항).

- 명백히 제정법상의 의무이어야 할 필요는 없다. 해당 법을 준수해야 하는 사람들이 법의 적용을 예상할 수 있을 정도로 그 의무가 명확하면 국회 또는 의회에서 제정한 법률이 아니라도 된다(전문 제41항). 따라서 관습법(common law) 상의 명백한 의무도 법적 의무에 포함된다.
- 또한 이것은 구체적으로 별도의 개인정보 처리를 요구하는 법적 의무규정이 있어야 한다는 것을 의미하는 것도 아니다. 법령이나 관습법에 명확히 근거를 둔 법적 의무를 준수하기 위한 목적이라면 법적 의무 준수를 위한 처리로 볼 수 있다.

⇒ 사례

고용주는 세무당국에 근로자의 급여 내역을 공개해야 하는 법적 의무를 준수하기 위해 개인정보를 처리할 필요가 있다. 고용주는 의무 입증을 위해 법적 의무 사항이 설명되어 있는 국세청 웹사이트에 링크를 걸어 둘 수 있다. 이와 같은 상황에서는 구체적으로 해당 법령의 조문을 인용할 필요는 없다.

⇒ 사례

금융회사는 서비스 이용자가 돈세탁에 관여하고 있거나 시도하고 있는 것으로 의심될 때 범죄 수사당국에 의심스러운 활동보고서를 제출해야 할 의무가 있다. 이 경우 법적 의무를 준수하기 위한 처리로 볼 수 있다.

⇒ 사례

법원의 명령으로 특정 목적을 위해 개인정보를 처리해야 할 때가 있다. 이 경우에도 법적 의무 준수를 위한 개인정보 처리로 볼 수 있다.

⇒ 사례

공정거래위원회는 공정거래법에 따라 불공정 거래에 대한 시정명령을 내릴 수 있다. 경우에 따라 이와 같은 권한 행사를 위해 개인정보의 처리가 요구된다. 사업자가 당국의 자료제출 명령에 따라 고객 데이터를 제공하는 것은 법적 의무 준수를 위한 개인정보 처리로 볼 수 있다.

2.4.3 법적 의무 준수를 위해 ‘필요한(Necessary)’ 경우의 의미

- 법적 의무를 준수하기 위해 개인정보 처리가 ‘반드시 필요한 것’이라고까지 요구하지는 않는다. 그러나 법적 의무 달성을 위하여 합리적이고 비례적인 방법이어야 한다. 개인정보를 처리할지 여부에 대해서 컨트롤러에게 재량권이 있거나 법적 의무 준수를 위한 다른 합리적인 방법이 있다면 법적 의무 준수를 합법처리의 근거로 적용할 수 없다.
- 대부분의 경우 법적 의무 준수를 위해 개인정보 처리가 필요한지 여부 및 필요하다면 어떤 개인정보가 어느 정도 필요한지 여부에 대해서는 해당 법령에 의해서 밝혀질 수 있다.

2.4.4 법적 의무를 합법처리의 근거로 할 때 주의할 사항

- 법적 의무에 근거하여 개인정보를 처리할 경우 정보주체는 삭제권, 개인정보 이동권, 반대권을 행사할 수 없다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제6조(처리의 합법성)제1항(c)■ 전문 제41항, 제45항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제15조(개인정보의 수집·이용)제1항제2호 및 제3호■ 제17조(개인정보의 제공)제1항제2호■ 제18조(개인정보의 목적 외 이용·제공)제2항제2호, 제6호~제9호■ 제23조(민감정보의 처리) 제1항제2호■ 제24조(고유식별정보의 처리) 제1항제2호■ 제24조의2(주민등록번호 처리의 제한) 제1항제1호 및 제3호■ 제25조(영상정보처리기기의 설치·운영) 제1항제1호

2.5 중대한 이익



셀프 체크리스트

Self Check List

	예	아니오
• 중대한 이익 보호 목적의 민감정보 처리에 대한 기준을 마련하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 중대한 이익 보호를 합법처리의 근거로 삼은 것을 정당화 할 수 있는 이유를 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에 대한 고지사항에 중대한 이익 보호의 목적과 그 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.5.1 개요

- 누군가의 생명을 보호하기 위해 개인정보를 처리해야 하는 경우 ‘중대한 이익(vital interests)’을 합법처리의 근거로 적용할 수 있다. GDPR은 정보주체나 다른 자연인의 중대한 이익을 보호하기 위해서 개인정보 처리가 필요하다고 규정하고 있다(제6조제1항(d)).

2.5.2 ‘중대한(vital)’ 이익의 의미

- GDPR에서 ‘중대한’ 이익은 매우 제한적으로 해석되고 있다. GDPR 전문은 중대한 이익에 대한 추가적인 지침을 제공하고 있는데 중대한 이익을 정보주체를 포함한 자연인의 생명(life)을 보호하기 위해 필요한 경우로 제한하고 있다(전문 제46항).
- 중대한 이익을 보호하기 위해 개인정보의 처리가 반드시 필요해야 한다. 합리적으로 개인정보를 처리하지 않거나 개인정보를 덜 침해하는 방법으로 중대한 이익을 보호할 수 있다면 중대한 이익을 개인정보 처리를 위한 합법적 근거로 삼을 수 없다.
- 정보주체가 동의를 할 수 있는 상황에서 중대한 이익 보호 목적의 개인정보 처리에 동의를 거부하였다면 건강정보를 포함한 민감정보는 중대한 이익 보호를 이유로 처리할 수 없다.

2.5.3 중대한 이익이 적용된 경우

- 중대한 이익은 주로 의료 목적을 위해 개인정보를 처리해야 하지만 정보주체가 이에 동의할 수 없는 경우에 적용된다. 특히 응급의료와 관련이 깊다.

⇒ 사례

심각한 교통사고를 당한 환자가 생명이 위태로운 상태로 병원에 입원했다. 환자의 중대한 생명 상의 이익을 보호하기 위해서는 정보주체의 진료기록을 해당 병원에 공개하는 것이 필요하다.

- 일반적으로 미리 계획되어 있는 병원진료에 대해서는 중대한 이익이 적용될 가능성이 희박하다. 이런 경우에는 공적 업무 수행, 적법한 이익 보호, 계약 이행 등과 같은 다른 합법처리의 근거가 더 적합하다.
다른 사람의 중대한 이익을 보호하기 위해 정보주체의 개인정보를 처리해야 하는 경우는 더욱 드물게 발생한다. 예를 들어, 자녀의 중대한 이익을 보호하기 위해 부모의 개인정보를 처리할 필요가 있는 경우가 이에 해당할 수 있다.
- 또한 중대한 이익은 대규모 개인정보 처리에 대해서는 합법처리를 위한 기준으로 삼기 어려운 경우가 많다. 다만, 전염병 감시와 같은 인도주의적 목적으로 개인정보를 처리하는 경우나 대규모 인명피해를 야기하는 자연재해 또는 인공재난이 발생한 경우에는 중대한 이익이 적용될 수 있다(전문 제46항).
- 그러나 다른 사람의 생명을 보호하기 위해 정보주체의 개인정보를 처리하는 것이 합법처리의 근거가 될 수 있는지 명백하지 않을 경우에는 일반적으로 ‘적법한 이익’ 등과 같은 다른 합법처리의 근거를 찾는 것이 바람직하다(전문 제46항).

2.5.4 중대한 이익을 합법처리의 근거로 할 때 주의할 사항

- 중대한 이익은 자연인의 생명 보호를 위한 개인정보의 처리 근거이므로 대부분 건강정보 처리와 관련된 가능성이 높다. 그런데 GDPR은 건강정보를 포함한 민감정보의 처리에 대해서는 별도의 처리 요건을 규정하고 있다.
- 즉, 자연인의 중대한 이익을 보호하기 위해 개인정보의 처리가 허용되는 경우에도 건강정보를 포함한 민감정보의 처리에 대해서는 별도의 요건이 충족되어야 한다. 민감정보는 정보주체가 물리적으로 또는 법적으로 동의를 줄 수 없는 경우에만 다른 사람의 중대한 이익 보호를 위한 목적으로 처리할 수 있다(제9조제2항(c)).
이것은 많은 경우에 민감정보의 처리에 대해서는 명시적 동의가 더 적절하다는 것을

의미한다. 바꿔 말하면 정보주체가 민감정보의 처리에 대한 동의를 거부할 경우 중대한 이익은 민감정보의 처리를 위한 합법처리의 근거가 되기 어렵다는 것을 의미한다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제6조(처리의 합법성)제1항(d) ■ 제9조(민감정보의 처리)제2항(c) ■ 전문 제46항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제15조(개인정보의 수집·이용)제1항제5호 ■ 제17조(개인정보의 제공)제1항제2호 ■ 제18조(개인정보의 목적 외 이용·제공) 제2항제3호 ■ 제24조의2(주민등록번호 처리의 제한)제1항제2호

2.6 공적 업무 수행



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보를 처리하기 전에 개인정보 처리가 필요한 공적 업무들을 파악·확인하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 공적 업무 수행을 위해 필요한 범위 내의 개인정보만 처리하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 공적 업무 수행을 합법처리의 근거로 삼은 것을 정당화 할 수 있는 이유를 문서화하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에 대한 고지사항에 공적 업무 수행 목적과 그 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.6.1 개요

- 공공기관 등이 공적 업무(public task) 수행이나 공적 권한 행사를 위해 개인정보 처리가 필요한 경우 ‘공적 업무’ 수행을 합법처리의 근거로 적용할 수 있다. GDPR은 공

익을 위한 업무의 수행이나 컨트롤러에게 부여된 공적 권한의 행사를 위해서는 개인정보 처리가 필요하다고 규정하고 있다(제6조제1항(e)).

- ‘공적 업무’의 수행이란 법에 규정된 공익을 위한 업무 수행뿐만 아니라 법에 규정된 공적 직무 및 권한의 행사도 포함하는 것이다. 이 경우 ‘공적 업무’ 수행은 주로 공공기관과 관련이 많지만 공공기관이 아니라도 공익을 위해 공권력을 행사하거나 공적 업무를 수행하는 모든 조직에 적용될 수 있다.
- 개인정보를 처리하기 위한 제정법 상의 권한이 필요한 것은 아니지만 컨트롤러의 업무, 기능 및 권한은 법에 명확한 근거를 두고 있어야 한다.
또한 공적 업무 수행을 위해 개인정보 처리가 반드시 필요해야 한다. 합리적으로 개인정보를 처리하지 않거나 또는 개인정보 침해가 덜한 방법으로 공적 업무를 수행할 수 있는 경우라면 공적 업무는 합법처리의 근거가 될 수 없다.

2.6.2 ‘공적 업무’의 의미

- 다음 중 어느 하나의 경우라면 ‘공적 업무’에 해당할 수 있다.
 - 법에 규정된 공익을 위한 업무를 수행하는 경우
 - 법에 규정된 공적 권한(공공기관의 업무, 기능, 의무, 권한)을 행사하는 경우
- 공공기관 등에게 주어진 권한(재량권을 포함)의 행사이면 되고 추가적으로 그 업무가 공공의 이익을 위한 것인지 여부는 판단하지 않는다. 그러나 공적 업무를 수행하기 위하여 그 개인정보의 처리가 꼭 필요한 것임을 입증할 수 있어야 한다.
이 경우 ‘필요하다’는 것이 의미하는 것은 개인정보 처리가 공적 업무의 수행 목적에 표적화되어 있고 비례적이라는 것을 의미한다. 동일한 결과를 달성하기 위하여 보다 합리적이고 개인정보를 덜 침해하는 다른 방법이 있다면 그것은 합법처리의 근거가 될 수 없다.

2.6.3 ‘법으로 규정한’의 의미

- ‘공적 업무’ 수행을 개인정보 처리에 대한 합법처리의 근거로 적용하기 위해서는 해당 업무, 기능, 의무, 권한 등이 EU법이나 회원국법으로 규정되어 있어야 한다. 따라서 그와 같은 업무의 대부분은 제정법 상의 업무라고 할 수 있다.
그러나 법의 적용이 명확하고 예측 가능하다면 반드시 제정법으로 규정되어 있는 업무에 한정할 필요는 없다. 법령이나 지침에서 규정하고 있는 업무 이외에 관습법에 의한 업무, 기능, 권한 등도 명확하다면 공적 업무에 포함된다(전문 제41항).

특별히 개인정보 처리를 위한 법적 권한은 필요하지 않다. 개인정보 처리의 목적이 공적 업무를 수행하거나 공적 권한을 행사하기 위한 것이라면 충분하다. 다만, 전반적인 업무 및 권한이 법률상 명확한 근거를 가지고 있어야 한다.

2.6.4 공공기관 등의 범위

- 공적인 권한을 행사하거나 공공의 이익을 위해 특정 업무를 수행하는 조직이면 모두 포함된다. 즉 ‘공적 업무’ 수행을 위한 합법처리의 요건은 조직의 성격이 아니라 조직의 기능에 초점이 맞추어져 있다.

⇒ 사례

한국수자원공사 등과 같은 공공기업은 행정기관은 아니지만 법령에 따라 공적인 업무를 수행하므로 공공기관 등에 포함될 수 있다.

2.6.5 공적 업무를 합법처리의 근거로 할 때 주의할 사항

- 컨트롤러가 개인정보를 ‘공적 업무’ 수행을 근거로 하여 처리하고 있는 경우 정보주체는 삭제권과 개인정보 이동권을 행사할 수 없다. 다만, 정보주체는 개인정보 처리에 반대할 수 있는 반대권은 행사할 수 있다.
- 공공기관이라도 법에 명시되어 있는 업무, 기능, 권한 등의 행사를 위해 개인정보 처리가 필요하다는 확신이 없다면 다른 합법처리의 근거를 찾아야 한다. 일반적으로 공공기관은 정보주체의 ‘동의’와 ‘적법한 이익’을 합법처리의 근거로 삼는 것에 상당히 제한을 받지만, 경우에 따라서는 공공기관도 ‘동의’와 ‘적법한 이익’을 합법처리의 근거로 삼을 수 있다. 특히 공권력 행사와 관련이 없는 업무라면 ‘동의’와 ‘적법한 이익’을 합법처리의 근거를 삼을 수 있다.
- 공공기관이라도 ‘공적 업무’의 수행과 관계없이 공익에 대한 기록 목적, 과학적 연구 목적, 통계 목적을 위한 개인정보 처리에 대해서는 합법처리의 근거가 필요하지 않다. ‘공적 업무’ 수행을 위한 개인정보 처리의 경우에도 책임성과 투명성 원칙을 준수하여야 한다. 즉, 법령 또는 관습법에서 공적 업무, 기능, 권한, 근거를 확인해야 하고, 공적 업무를 수행하기 위해 개인정보 처리가 필요하다고 결정한 내용을 문서화해야 하며, 정보주체에 대한 고지사항(privacy notice)에 처리의 목적 및 합법처리의 근거를 포함해야 한다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제6조(처리의 합법성)제1항(e) 및 제3항■ 전문 제41항, 제45항, 제50항 참조
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제15조(개인정보보호 원칙)제1항제3호■ 제17조(개인정보의 제공)제1항제2호■ 제18조(개인정보의 목적 외 이용·제공 제한) 제2항제7호~제9호

2.7 적법한 이익 추구



셀프 체크리스트

Self Check List

	예	아니오
• 적법한 이익이 처리를 위한 가장 적절한 근거라는 것을 확인하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 적법한 이익을 처리의 근거로 삼은 것을 정당화할 수 있는 이유를 문서화 하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 적법한 이익 추구를 위한 최소한의 개인정보만 처리하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에 대한 고지사항에 적법한 이익 추구의 목적과 그 근거를 포함하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.7.1 개요

- 컨트롤러는 ‘적법한 이익(legitimate interests)’을 개인정보 처리를 위한 합법처리의 근거로 삼을 수 있다. 적법한 이익은 개인정보 처리를 위한 가장 유연한 법적 근거이지만 항상 적절하다고는 할 수 없다.
‘적법한 이익’은 사람들이 합리적으로 예상할 수 있고 사생활 침해에 미치는 영향을 최소화하는 방법으로 개인정보를 처리하거나 개인정보의 처리가 정당함을 충분히 설득할 수 있는 경우에 가장 적절한 ‘합법처리’의 근거가 될 수 있다.
- 컨트롤러가 ‘적법한 이익’을 합법처리의 근거로 선택한 경우에는 정보주체의 권리와 이익을 고려하고 보호해야 할 추가적인 책임을 부담한다. ‘적법한 이익’으로 인정받기 위

해서는 다음 3가지 요소를 충족하여야 한다.

- 적법한 이익이 존재한다는 것을 확인할 것
- 처리가 적법한 이익을 달성하기 위해 필요하다는 것을 보여줄 것
- 정보주체의 이익, 권리 및 자유와 균형을 이룰 것

이 경우 ‘적법한 이익’에는 자신이 추구하는 이익뿐만 아니라 제3자가 추구하는 이익도 포함될 수 있다. 또한 상업적 이익이나 개인적 이익뿐만 아니라 더 나아가 사회적 이익도 포함된다.

- 컨트롤러의 이익은 정보주체의 이익과 균형을 이루어야 한다. 만약 정보주체가 그와 같은 처리를 합리적으로 예상할 수 없다면 또는 그와 같은 처리가 정보주체에게 부당한 해를 끼친다면 정보주체의 이익이 컨트롤러의 이익에 우선하는 것으로 평가될 수 있다. 적법한 이익을 위한 처리로 인정받기 위해서는 개인정보 처리가 반드시 필요해야 한다. 합리적으로 판단해 개인정보를 처리하지 않는 방법으로 또는 개인정보를 덜 침해하는 방법으로 적법한 이익을 달성할 수 있다면 ‘적법한 이익’은 합법처리의 근거가 될 수 없다.
- 공공기관이 자신의 직무 수행을 위하여 개인정보를 처리하는 경우에는 원칙적으로 ‘적법한 이익’을 합법처리의 근거로 활용할 수 없으나 공적 권한 행사와 무관한 목적을 위하여 개인정보를 처리하는 경우에는 적법한 이익을 합법처리의 근거로 적용할 수 있다.

2.7.2 적법한 이익의 의미

- GDPR은 ‘적법한 이익’에 대하여 구체적인 정의를 두고 있지는 않지만, 정보주체의 이익이나 기본적 권리와 자유가 우선하는 경우를 제외하고 컨트롤러 또는 제3자의 적법한 이익을 추구하기 위해서 개인정보 처리가 필요한 경우를 규정하고 있다(제6조제1항(f)).

이에 따라 ‘적법한 이익’으로 인정받기 위해서는 아래 3가지 기준을 충족해야 한다.

- 목적 : 적법한 이익을 추구하고 있는가?
- 필요성 : 목적을 위해 개인정보 처리가 필요한가?
- 이익형량 : 적법한 이익이 정보주체의 이익에 우선하는가?

- 이 경우 ‘필요하다’가 의미하는 것은 처리가 목표 달성에 표적화되어 있고 비례적이어야 한다는 것을 의미한다. 동일한 결과를 얻기 위해 개인정보를 덜 침해하는 다른 합리적인 방법이 있다면 ‘적법한 이익’으로 인정받기 어렵다.

- 컨트롤러의 이익은 정보주체의 이익과 균형을 이루어야 한다. 정보주체들이 개인정보가 이용되는 것에 대해 합리적으로 예상하지 못했거나 개인정보 처리가 정보주체들에게 부당한 피해를 야기할 수 있다면 정보주체의 이익이 컨트롤러의 이익에 우선한 것으로 평가될 수 있기 때문에 ‘적법한 이익’으로 보기 어렵다.

GDPR에서는 다양한 이익들이 ‘적법한 이익’에 포함될 수 있다. 컨트롤러 자신의 이익뿐만 아니라 제3자의 이익도 포함될 수 있고, 상업적 이익뿐만 아니라 사회적 이익도 포함될 수 있다.

- GDPR은 마케팅, 부정행위 방지, 그룹 내 개인정보 이전, IT 보안 등을 위한 고객 또는 근로자 개인정보의 이용을 잠재적인 ‘적법한 이익’으로 언급하고 있지만 적법한 이익이 이것에만 한정되는 것은 아니다. 또한 GDPR은 잠재적인 범죄 행위나 보안 위협에 관한 정보를 당국에 제공하는 것도 적법한 이익으로 보고 있다.

2.7.3 적법한 이익이 적용되는 경우

- ‘적법한 이익’은 사람들이 합리적으로 예상하는 방식으로 그리고 사생활에 미치는 영향을 최소화한 방식으로 개인정보를 처리할 때 적용될 수 있다. 또한 개인정보 처리가 정보주체에게 어떤 영향을 미치더라도 개인정보를 처리하는 것이 컨트롤러나 제3자에게 훨씬 더 이익이 크다면 그 처리는 정당화될 수 있다.

개인정보를 이용하는 방법이 비례적이고, 프라이버시에 미치는 영향도 최소한에 그친 경우, 정보주체가 충분히 예상할 수 있거나 반대할 가능성이 없다는 것을 보여줄 수 있다면 마케팅 활동도 적법한 이익이 될 수 있다.

- 아동의 개인정보를 처리하는 경우에도 ‘적법한 이익’을 적용할 수는 있지만, 아동의 이익이 보호되도록 각별히 주의해야 한다.

제3자에게 개인정보를 제공할 때에도 ‘적법한 이익’을 적용할 수 있다. 이 경우 컨트롤러는 제3자가 무슨 이유로 개인정보를 원하는지, 실제로 제3자가 그 개인정보를 필요로 하는지, 그들이 그것을 가지고 무엇을 할지를 고려해야 하며 제3자 제공이 정당하다는 것을 입증해야 한다.

- 사람들이 이해할 수 없고 합리적으로 예상할 수 없는 방식으로 개인정보를 이용하거나 제공할 경우 반대할 사람들이 있을 것으로 생각한다면 ‘적법한 이익’을 합법처리의 근거로 삼는 것은 피해야 한다. 또한 정보주체에게 미치는 영향을 정당화할 수 있는 강력한 이유가 있다고 확신하지 않는 한 정보주체에게 해를 끼칠 수 있는 처리는 ‘적법한 이익’에 근거해서 처리해서는 안 된다.

- 공공기관은 원칙적으로 공적 업무를 수행하기 위한 목적의 개인정보 처리에 대해서는 ‘적법한 이익’을 합법처리의 근거로 할 수 없다. 그러나 공공기관이 공적 업무 목적 외의 다른 정당한 이유가 있다면 ‘적법한 이익’을 합법처리의 근거로 고려할 수 있다. 공공기관이 상업적 이익을 가진 경우가 이에 해당할 수 있다.

2.7.4 적법한 이익을 실무에 적용하는 방법

- 컨트롤러가 개인정보 처리를 ‘적법한 이익’에 의존하고 싶다면 3단계 테스트를 통해 미리 적용 가능성을 평가해 보는 것이 바람직하다. 이것을 ‘적법한 이익 평가(LIA, Legitimate Interests Assessment)’라고 부른다. LIA에 대해서는 적법한 이익 추구에 해당하는지 여부를 판단하기 위한 이익형량 가이드¹⁴를 참조할 수 있다.
- LIA는 구체적 정황과 상황에 기반한 일종의 위험평가이다. LIA는 개인정보 처리가 적법하다는 것을 입증하는데 도움이 되고, GDPR 제5조제2항 및 제24조에 따른 책임성 원칙의 준수를 입증하는데도 도움이 된다. LIA는 아래와 같이 3단계 평가로 구성되어 있다.
- [1단계] 목적테스트
 - 개인정보를 처리하려는 이유가 무엇인가? - 달성하고자 하는 목표가 무엇인가?
 - 처리를 통해 이익을 얻는 사람은 누구인가?
 - 처리를 통해 얻을 수 있는 광범위한 공익이 존재하는가?
 - 그와 같은 혜택이 얼마만큼 중요한가?
 - 개인정보를 처리하지 못할 경우 어떤 영향이 있을 것인가?
 - 개인정보의 이용이 비윤리적이거나 불법적이지 않은가?
- [2단계] 필요성 테스트
 - 개인정보 처리가 실제로 이익을 확대하는 데 도움이 되는가?
 - 개인정보 처리 방법이 타당한가?
 - 사생활을 덜 침해하는 다른 방법이 있는가?
- [3단계] 이익형량 테스트
 - 정보주체와 어떤 성격의 관계를 맺고 있는가?
 - 특별히 민감하거나 사적인 개인정보가 포함되어 있는가?
 - 정보주체는 자신의 개인정보가 어떤 방법으로 이용될 것으로 예상하고 있는가?

14 제29조 작업반, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC(WP217), 2014. 04. 09.

- 정보주체에게 처리하는 방법을 충분히 설명하고 있는가?
 - 누군가 처리에 반대하거나 권리를 침해받았다고 주장할 가능성이 있는가?
 - 정보주체에게 어떤 영향을 미칠 수 있는가?
 - 정보주체에게 미칠 수 있는 영향은 얼마나 큰가?
 - 아동의 개인정보를 처리하고 있는가?
 - 정보주체 중 취약계층이 있는가?
 - 영향을 최소화할 수 있는 안전조치를 취할 수 있는가?
 - 탈퇴 또는 거부를 할 수 있는 방법을 제안하고 있는가?
- LIA가 끝나면 ‘적법한 이익’이 합법처리의 근거가 될 수 있는지 여부를 결정하고 그 결과를 기록해 두어야 한다. LIA를 통해서도 결과에 대해 확신이 서지 않는다면 다른 합법처리의 근거를 찾는 것이 안전하다. LIA 결과 중대한 위험이 식별되었다면 개인정보 영향평가(DPIA)를 고려해야 한다.

2.7.5 적법한 이익을 합법처리의 근거로 할 때 주의할 사항

- 1 단계 : 제7조(a)~(f)에 따라 잠재적으로 적용될 수 있는 합법처리의 근거를 평가한다.

2 단계 : 추구하는 이익이 합법적인 것인지 불법적인 것인지를 여부를 결정한다.

3 단계 : 개인정보 처리가 추구하고자 하는 이익을 달성하기 위해 필요한 것인지 여부를 결정한다.

4 단계 : 컨트롤러의 이익이 정보주체의 기본적 권리 또는 이익보다 우선하는지 여부를 평가하여 잠정적으로 양자 간의 균형을 확보한다.

5 단계 : 추가적인 보호 조치를 고려하여 최종적으로 양자 간의 균형을 확보한다.

6 단계 : 규정의 준수를 증명하고 투명성을 보장한다.

7 단계 : 정보주체가 개인정보 처리에 대하여 반대권을 행사한 경우 어떻게 할지에 대해서 미리 검토한다.

- 정보주체에 대한 고지사항에 개인정보를 처리하는 근거가 ‘적법한 이익’이라는 사실을 알리고 그 이익이 무엇인지도 알려야 한다. 또한 새로운 목적을 위해 개인정보를 처리하기를 원한다면 그것이 양립할 수 있는 것인지 여부를 판단해야 한다.

컨트롤러가 ‘적법한 이익’에 근거해서 개인정보를 처리할 경우 정보주체는 개인정보 이동권을 행사할 수 없다. 그러나 직접 마케팅을 위한 개인정보 처리의 근거를 ‘적법한 이익’에 두고 있다면 정보주체의 반대권은 절대적 권리이므로 즉시 처리를 중단해야 한다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제6조(처리의 합법성)제1항(f) ■ 전문 제47항~제49항 ■ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC(WP217), WP29
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제15조(개인정보의 수집·이용)제1항제6호



동의



Point

- 동의의 유효 요건에 대해서 이해할 수 있다.
- 명시적 동의가 필요한 경우와 그 획득 방법을 알 수 있다.



셀프 체크리스트

Self Check List

	예	아니오
동의 방법		
• 동의가 가장 적합한 합법처리의 근거임을 확인하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 약관과 구분해서 별도로 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 이해하기 쉽고 간결하고 명확하고 평이한 언어로 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의를 서비스 제공의 전제조건으로 삼지 않고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 처리 목적·유형별로 구체적·개별적인 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
동의 기록		
• 동의 받은 날짜와 방법을 기록해 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체에게 알린 내용을 기록해 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
동의 관리		
• 정기적으로 동의서를 검토해서 변경 사항을 체크·반영하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 아동정보, 민감정보, 범죄정보의 처리에 대한 별도의 절차를 마련해두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의 철회 방법을 공개하고 언제든지 쉽게 철회할 수 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 동의 철회에 대해 불이익을 주지 않고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

3.1 동의를 정의

- ‘동의(consent)’란 정보주체가 진술 또는 행동을 통하여 자신의 개인정보 처리에 대한 긍정의 의사(합의)를 표현하는 것을 의미한다. 즉, 개인정보 처리에 대한 정보주체의 자유로운 승낙의 의사표시를 의미한다는 것이다. 이때 정보주체의 동의는 ‘진정한(genuine)’ 것이어야 하며, 이는 형식적인 요건의 충족만으로 달성할 수 없다. 특히 기망, 강요, 협박, 불이익 등과 같은 요소가 있는 경우 그 같은 상황에서의 동의는 자유로운 것이 아니므로 유효한 동의가 될 수 없다.
- 또한 동의는 특정되어 있어야 하고(specific), 충분한 정보가 제공된 상태에서 이루어져야 하며(informed), 의사표시가 모호하지 않아야 한다(unambiguous).

3.2 동의의 유효 요건

3.2.1 자유로운 동의¹⁵

- ‘자유로운(free/freely given) 동의’란 정보주체에게 자신의 개인정보 처리에 대하여 실질적인 선택권과 통제권을 부여하는 것을 의미한다. 정보주체가 반드시 동의하여야 한다는 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 상황에서의 동의는 합법처리의 근거로 삼을 수 없다. 또한 개인정보 처리에 대한 동의는 ‘이용 약관(general terms and conditions)’에 포함되어 제시해서는 안 된다(제7조제4항¹⁶, 전문 제43항¹⁷).

15 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.5~10.

16 ‘동의를 자유롭게 부여되는지를 평가할 때, 서비스 제공을 포함한 계약 이행이 그 계약의 이행에 필요하지 않은 개인정보 처리에 대한 동의를 조건으로 하지 않는지 세심하게 살펴야 한다.’

17 ‘서비스 제공을 포함한 계약 이행에 동의가 필요하지 않음에도 불구하고 동의에 의존하는 경우, 동의가 자유로이 부여되지 않는 것으로 본다.’

예시

서비스를 이용하기 위해서 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 동의 철회에 따른 비용이 발생하지 않는 다거나, 동의 철회에 대하여 강압이나 기망 등 중대한 부정적 결과가 발생하지 않는다는 것을 입증할 수 있는 경우 동의를 자유롭게 제시되었음을 증명하는 데에 도움이 될 수 있다.

3.2.2 개별적으로 특정된 동의¹⁸

■ 개인정보 처리에 대한 정보주체의 통제권과 투명성을 보장하기 위하여 동意的 내용은 개별적으로 특정(specific)되어야 한다. 개별적으로 특정한 동의의 요건을 충족하기 위하여 컨트롤러는 다음 사항을 적용하여야 한다.

- ① 기능 확대(function creep) 현상¹⁹에 대비한 안전조치로써 목적을 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 한다는 것을 의미한다. 즉 정보주체는 특정 목적에 대하여 해당하는 특정 동의를 제공할 수 있어야 한다. 따라서 목적별로 선택해서 동의할 수 있도록 조치하지 않고 일괄적으로 받은 동의는 효력이 없다.

¹⁸ 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.11~12.
¹⁹ 기능 확대(function creep) 현상: 프로젝트가 시작한 시점 이후 프로젝트의 범위가 지속적으로 또는 통제되지 않은 채 확대되는 현상.

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.

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 동의²⁰

- GDPR은 동의 조건으로 정보주체에게 동의에 필요한 충분한 정보를 제공해야 한다는 점(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 GDPR 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
- 다만 이 중 ① 또는 ⑥에 대한 정보는 개인정보처리방침(privacy policy)에 포함되어

20 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.12~14.

제시될 수 있다.

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 표시²¹

- 동의는 반드시 개인정보 처리 활동이 발생하기 전에 획득되어야 하며(opt-in), 정보주체가 동의하였다는 사실과 동의한 내용이 분명해야 한다(unambiguous indication). 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 의미한다. 그러나 아래의 경우에는 동의를 위한 명확한 표시로 인정될 수 없다.
 - ① 사전에 선택되어 있는 체크박스(pre-ticked boxes)를 제시하는 것
 - ② 침묵(silence)이나 부작위(inactivity)를 동의로 보는 것
 - ③ 서비스가 제시하는 절차를 동의 의사 표시 없이 단순히 진행하는 것
 - ④ 이용약관에 포괄적인 수용(이른바 ‘blanket acceptance’)의 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·공정적 동작(active affirmative motion)으로 효력을 갖기 위하여 서비스 이용에 어느 정도 지장을 주는 것은 불가피할 수 있다.

21 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.15~17.

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 철회 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 동의가 필요한 경우²²

- GDPR은 중대한 개인정보보호 위험이 발생하여 정보주체에게 개인정보에 대한 높은 수준의 통제권이 필요하다고 보는 경우 정보주체의 명시적 동의(explicit consent)를 요구하고 있다.
- ‘명시적(explicit)’이란 정보주체가 동의를 표현하는 방식을 의미하는데 정보주체의 의사 표시가 명확해야 한다는 것을 말한다. 구체적인 방법으로는 서면진술, 동의 의사가 표명된 이메일 발송, 정보주체의 서명이 포함된 스캔 문서의 업로드, 전자 서명 요구, 동의에 대한 2단계 검증 등이 있다.

22 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.18~20.

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.
- [명시적 동의 예] 웹사이트 운영자가 사이트 방문자에게 '나는, OO 웹사이트가 나의 개인정보를 처리하는 것에 동의합니다.(I, hereby, consent to the processing of my data)'라는 문구와 함께 'Yes ☐ / No ☐

3.4 동의의 철회²³

- 동의의 철회(withdrawal of consent)는 GDPR에서 정보주체의 권리 행사에 중요한 위치를 차지하며, 컨트롤러는 정보주체가 동의를 제공할 때와 마찬가지로 언제든지 철회할 수 있도록 보장하여야 한다(제7조제3항). GDPR은 동의의 철회 행위가 동의의 제공 행위와 반드시 동일해야 한다고 설명하지는 않는다. 그러나 만약 컨트롤러가 한번의 마우스 클릭이나 스와이프 또는 키 누름 등의 전자적 수단으로 쉽게 동의를 획득하는 경우 동의의 철회 역시 그와 같은 방식으로 쉽게 이루어질 수 있어야 한다.

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 영업시간 중에 전화를 걸어야 하는데, 이는 휴일 없이 24시간 열려 있는 온라인 티켓 대행사를 통하여 동의하는 데 필요한 한 번의 마우스 클릭보다 더 번거롭기 때문이다.

23 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.21~23.

GDPR 관련 규정

- 제4조(정의)제11항
- 제6조(처리의 합법성)제1항(a)
- 제7조(동의의 조건)
- 제9조(민감정보의 처리)제2항(a)
- 제22조(프로파일링을 포함한 자동화된 의사결정)
- 제49조(특정 상황에 대한 역외 이전 예외 조항)
- 전문 제32항, 제38항, 제40항, 제42항, 제43항, 제171항

한국 개인정보보호법 관련 규정

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



아동 개인정보



Point

- ‘아동’ 및 ‘법정대리인’의 권리를 이해할 수 있다.
- 아동 개인정보를 처리할 때 준수하여야 하는 개인정보 처리 규정을 이해할 수 있다.



셀프 체크리스트

Self Check List

	예	아니오
• GDPR 적용 대상 국가별 친권자 동의가 필요한 아동 연령기준을 파악하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 아동 개인정보를 처리하기 위하여 동의를 받아야 할 때에는 부모 등 친권자의 동의를 받고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 아동이 쉽게 이해할 수 있도록 간결하고 평이한 언어를 사용하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 아동의 연령을 검증할 수 있는 합리적인 절차를 두고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.1 개요

- GDPR은 아동의 경우 개인정보 처리에 따른 위험성과 그 결과 그리고 자신의 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.²⁴

24 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.23~24.

4.2 아동에게 제공되는 온라인 서비스

- GDPR 제8조 제1항은 만 16세 미만의 ‘아동에게 직접’ 정보사회서비스(information society services)를 제공할 때는 부모 등 친권을 보유하는 자(holder of parental responsibility)의 동의를 받도록 규정하고 있다. 다만, GDPR은 정보사회서비스 제공자가 잠재적 고객에게 해당 서비스가 성인에게만 제공되는 것임을 명확히 하고, 이러한 사실이 사이트의 콘텐츠나 마케팅 계획 등 다른 요소에도 위배되지 않는 경우 해당 서비스는 ‘아동에게 직접’ 제공되는 것이 아닌 것으로 판단한다.
- GDPR은 아동의 연령을 만 16세 미만으로 규정하고 있으나 회원국은 자국의 법률을 통하여 친권자 등의 동의를 요하는 아동의 연령 기준을 만 13세까지 낮추어 규정할 수 있다.

표 3. EU 회원국의 친권자 동의가 필요한 아동 연령²⁵

기준 연령	해당 국가
만 13세	벨기에, 덴마크, 에스토니아, 핀란드, 라트비아, 몰타, 포르투갈, 스웨덴
만 14세	오스트리아, 불가리아, 사이프러스, 이탈리아, 리투아니아, 스페인
만 15세	체코, 프랑스
만 16세	크로아티아, 독일, 그리스, 헝가리, 아일랜드, 룩셈부르크, 네덜란드, 폴란드, 루마니아, 슬로바키아, 슬로베니아

※ 위 내용은 2019년 10월 기준이므로 이후 변동될 수 있음.

4.3 친권자 동의²⁶

- 동의를 바탕으로 아동에게 정보사회서비스를 제공하는 경우, 컨트롤러는 아동의 연령을 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.

25 Ingrida Milkaite and Eva Lievens, "Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU", Better Internet for Kids, 2020. 03. 17., <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751>

26 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.26~26.

- 동의를 제공하는 자가 동의를 표시할 수 있는 연령에 도달하였는지, 그리고 동의를 제공하는 자가 아동에 대한 부모의 책임을 보유한 자인지를 합리적으로 확인하는 방식은 개인정보 처리에 내재된 위험과 이용 가능한 기술에 따라 다르다.
- GDPR은 제8조 제2항에서 컨트롤러는 이용 가능한 기술을 고려하여 친권자가 개인정보 처리에 동의했는지 여부를 확인하기 위해 “합리적인 노력”을 하도록 요구하고 있다. 그러나 GDPR은 친권자의 동의 획득에 대해 실질적인 방법을 설명하지는 않는다. 이에 제29조 작업반은 컨트롤러의 노력이 합리적인지 여부와 관련하여 모든 상황에서 처리의 특성을 고려해야 한다고 설명하고 있다.²⁷ 따라서 처리의 위험이 적은 경우 예를 들어 명백하고 특정된 목적을 위해 아동으로부터 최소한으로 개인정보를 수집하는 경우, 컨트롤러는 처리의 위험이 큰 경우보다 더 낮은 수준의 친권자 동의 확인 방법을 고려할 수 있다.
 - 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.

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.

²⁷ 제29조 작업반, Guidelines on Consent under Regulation 2016/679, 2018. 04. 16., pp.23-27.

- 친권자가 제8조에 따라 아동의 개인정보 처리에 대한 동의를 한 경우 그 동意的 효력은 아동이 디지털 동의 연령에 도달한 이후에도 유효하다.
GDPR 제8조에도 불구하고 동의 이외에 다른 합법처리의 근거가 있는 경우에는 그 근거에 의해서 아동 개인정보를 처리할 수 있다.

4.4 친권자의 동의를 확인하는 방법²⁸

- 친권자의 동의를 확인하는 구체적인 방법은 매우 다양하다. 이메일 회신만으로 가능할 수도 있고 추가적인 증거가 필요할 수도 있다. 또한 친권자의 신용카드정보 또는 다른 결제수단정보에 의할 수도 있다.

참고

미국의 아동프라이버시보호법(COPPA)을 준수하기 위해 미국 FTC가 제시한 아래의 방법을 활용할 수도 있다.

- 동의서에 서명한 후 전자스캔, 우편, 팩스를 통해 다시 보내는 방법
- 신용카드, 직불카드, 그 밖의 온라인결제시스템을 이용하여 계정 소유자에게 각각의 개별거래에 대한 통지를 제공하는 방법
- 숙련된 직원이 무료로 전화를 걸어 전화로 동의를 받는 방법
- 화상회의를 통해 훈련된 직원과 연결하는 방법
- 정부가 발급한 신분증 사본을 제공받아 확인하는 방법(이 경우 확인절차가 종료되면 해당 정보를 반드시 삭제)
- 친권자가 아니면 답변할 수 없는 지식기반질문에 답변하게 하는 방법
- 얼굴 인식 기술을 이용하여 친권자가 제출한 친권자의 운전면허증 사진과 친권자가 제출한 다른 사진을 비교해서 확인하는 방법
- 이메일을 통해서 동의를 받고 부모에게 다시 확인하는 이른바 “이메일 플러스” 방법을 통해서 확인하는 방법
※ 아동의 개인정보가 오로지 내부 목적으로만 이용되고 외부에 공개되지 않아 위험이 낮은 경우 “이메일 플러스” 방식을 이용

28 CIPL, GDPR Implementation In Respect of Children's Data and Consent, 2018. 03. 06.

4.5 아동에 대한 통지²⁹

- GDPR 제12조 및 전문 제58항은 정보주체에게 제공하는 모든 정보는 간결하고 투명하며 쉬운 언어로 작성해야 한다고 규정하고 있다. 특히 아동을 대상으로 하여 제공되는 정보는 더욱 엄격한 기준을 적용하여야 한다.
- 따라서 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 보장해야 한다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제8조(정보사회서비스에 관한 아동의 동의에 적용되는 조건)■ 제6조(처리의 합법성)제1항(f)■ 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식)■ 제17조(삭제권) 제1항(f)■ 제22조(자동화된 의사결정)■ 제40조(행동규약)제2항(g)■ 제57조(감독기구의 업무)제1항(b)■ 전문 제38항, 제58항, 제65항, 제71항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제22조(동의를 받는 방법)제6항

29 ICO, Consultation: Children and the GDPR guidance, 2018



민감정보 및 범죄정보



Point

- 민감정보와 범죄정보의 개념과 범위에 대하여 이해할 수 있다.
- 민감정보 및 범죄정보의 처리 금지 원칙의 예외 조항에 대하여 이해할 수 있다.



셀프 체크리스트

Self Check List

	예	아니오
• 민감정보 또는 범죄정보를 임의 수집 및 보유하거나 처리하지 않는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 민감정보 또는 범죄정보를 처리하는 경우 명확한 법적 근거에 기반하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 유전자정보, 생체정보, 건강정보를 처리할 때에는 회원국법에 따른 추가 요건을 확인하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

5.1 민감정보의 처리 제한

5.1.1 개요

- GDPR은 해당 개인정보의 성격상 일반 개인정보에 비해 민감해서 특별한 보호가 필요한 정보를 ‘특수한 범주의 개인정보’로 규정하고 원칙적으로 처리를 금지하고 있다(제9조제1항).

이에 따라 민감정보를 적법하게 처리하기 위해서는 GDPR 제6조에 따른 합법처리의 요건만 충족해서는 안되고 그와 함께 제9조에서 규정하고 있는 민감정보 처리를 위한 추가적인 요건을 갖추어야 한다.

- 컨트롤러는 민감정보를 처리하기 전에 민감정보 처리에 대한 합법처리의 근거(정당성)를 마련하여 이를 문서화해야 한다.

5.1.2 민감정보의 개념

- GDPR상 ‘민감정보’란 인종·민족의 기원, 정치적 견해, 종교·철학적 신념, 노동조합의 가입 여부를 나타내는 개인정보의 처리와 유전자 정보, 개인을 고유하게 식별할 수 있는 생체정보, 건강정보, 성생활·성적 취향에 관한 정보를 의미한다(제9조제1항).
생체정보도 민감정보에 포함되나 모든 생체정보가 민감정보에 포함되는 것은 아니고 정보주체를 식별할 목적으로 이용되는 생체정보(지문, 홍채, 성문, 안면윤곽 등)만 민감정보로 보호를 받는다.
- 범죄정보는 GDPR 제10조에 의해서 별도로 보호를 받고 있기 때문에 제9조의 민감정보 처리에 관한 규정은 적용되지 않는다.
민감정보는 정보주체에 대한 불법적인 차별을 목적으로 이용되는 등 정보주체의 기본적인 권리와 자유에 보다 중요한 위험을 초래할 수 있기 때문에 별도의 보호가 필요하다.

5.1.3 민감정보의 처리

- 컨트롤러와 프로세서는 다음 경우에 한하여 민감정보를 처리할 수 있다(제9조제2항).
 - ① 정보주체의 명시적 동의(explicit consent)를 획득한 경우(다만 동의에 근거하는 것이 EU 또는 회원국 법률에 의해 금지되는 경우는 제외)
 - ② 고용, 사회안보, 사회보장 및 사회보호법(social security and social protection law) 또는 단체협약에 따른 의무의 이행을 위하여 필요한 경우
 - ③ 정보주체가 물리적 또는 법적으로 동의를 할 능력이 없는 경우에 정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위하여 필요한 경우
 - ④ 정치·철학·종교 목적을 지닌 비영리 단체나 노동조합이 하는 처리로, 회원이나 과거 회원(또는 그 목적과 관련하여 정기적인 접촉을 유지하는 자)에 관해서만 처리하며, 또한 동의 없이 제3자에게 공개하지 않는 경우
 - ⑤ 정보주체가 명백히 일반에게 공개한 정보를 처리하는 경우
 - ⑥ 법적 청구권의 설정, 행사, 방어 또는 법원이 재판 목적으로 처리하는 경우
 - ⑦ 중대한 공익을 위하여 또는 EU법이나 회원국법을 근거로 하는 처리로, 추구하는 목적에 비례하고 적절한 보호조치가 있는 경우
 - ⑧ EU법이나 회원국법 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

5.1.4 회원국법에 의한 특칙

- 회원국은 국내법으로 GDPR 제9조제4항에 따른 유전자정보, 생체정보, 건강정보의 처리에 대하여 추가 요건을 규정할 수 있다.

5.2 범죄정보의 처리 금지

5.2.1 개요

- GDPR은 민감정보와 범죄정보를 구분해서 규정하고 있다. 그러나 유럽평의회 108호 조약(CoE 108 Convention)³⁰은 범죄정보를 민감정보의 한 유형으로 보고 있다. 범죄정보의 처리는 정보주체에게 미치는 영향이 매우 크기 때문에 GDPR은 범죄정보를 민감정보와 구분해 보다 철저히 보호하고 있다.
- 범죄경력 및 범죄행위와 관련된 정보는 GDPR 제6조의 합법처리의 요건을 갖추었더라도 처리할 수 없는 경우가 많다(제10조). GDPR은 범죄정보를 처리할 수 있는 처리주체를 공적 권한을 갖고 있는 공공기관 등으로 제한하고 있기 때문이다.
따라서 범죄정보를 처리하려면 GDPR 제6조에 따른 합법처리의 요건과 제10조에 따른 법적 권한 또는 공적 권한을 둘 다 충족하여야 한다. GDPR 제9조에 따른 민감정보의 처리에 관한 규정은 범죄정보에는 적용되지 않는다.
- 컨트롤러는 범죄정보를 처리하기 전에 범죄정보 처리에 대한 합법처리의 근거(정당성)를 마련하여 이를 문서화해야 한다.

5.2.2 범죄정보의 범위

- ‘범죄정보’란 형사상 유죄판결 및 범죄행위와 관련된 정보를 의미한다. 이와 같은 범죄정보에는 범죄혐의, 범죄행위, 유죄판결 등에 관한 정보가 포함된다.
행정법상 과징금·과태료 처분이나 민사법상 손해배상판결은 범죄정보에 포함되지 않는다.

30 CoE(Council of Europe) 108 Convention(1981. 01. 28). CoE 각료이사회는 2018년 5월 18일에 기존 협약을 개정하는 의정서를 채택하고, 그해 6월 21일 연차총회에서 CoE 108+의 시행을 의결하였다.

5.2.3 범죄정보의 처리

- ‘범죄정보’를 처리하기 위해서는 제6조에 따른 합법처리의 조건과 함께 제10조에 따른 범죄정보의 처리요건을 갖추어야 한다. 그러나 범죄정보는 민감정보와 달리 정보주체의 동의가 있어도 처리할 수 없다. 법률상 범죄정보를 처리할 수 있는 공적 권한이 반드시 있어야 처리가 가능하다.
구체적으로 범죄정보는 아래와 같이 공적 권한이 존재하는 경우에만 처리가 가능하다.
 - ① 컨트롤러가 공적 권한의 통제 하에 있을 경우
 - ② 범죄정보의 보호를 위해 적절한 안전장치를 규정하는 EU법 또는 회원국법이 허가하는 경우
- 특히 범죄경력을 종합적으로 기록한 범죄경력 종합기록부는 공적 권한의 통제 하에서만 처리가 가능하다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제9조(민감정보의 처리)■ 제10조(범죄정보의 처리)■ 전문 제51항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제23조(민감정보의 처리 제한)



03

정보주체의
권리보장



1. 개요
2. 정보를 제공받을 권리(Right to be informed)
3. 정보주체의 접근권(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)



개요

- GDPR 제3장(정보주체의 권리)은 정보주체의 권리 행사와 강화에 대한 내용을 규정하고 있으며, 특히 삭제권(‘잊힐 권리’), 처리 제한권, 개인정보 이동권 등을 새로 도입하고 접근권, 삭제권(‘잊힐 권리’) 등의 대상을 확대하였다는 점에서 기존 Directive보다 정보주체의 권리 강화 내용을 구체화하였다는 것을 알 수 있다.

| 표 4. 정보주체의 권리 강화에 대한 내용 및 관련 주요 조문

No.	정보주체의 권리	관련 조문
1	정보를 제공받을 권리(Right to be informed)	제1절 제12조~제14조
2	정보주체의 접근권(Right of access by the data subject)	제2절 제12조, 제15조
3	정정권(Right to rectification)	제12조, 제16조, 제19조
4	삭제권(‘잊힐 권리’)[Right to erasure(‘Right to be forgotten’)]	제3절 제13조, 제17조, 제19조
5	처리 제한권(Right to restrict to processing)	제12조, 제18조, 제19조
6	개인정보 이동권(Right to data portability)	제12조, 제20조
7	반대권(Right to object)	제12조, 제21조
8	프로파일링을 포함한 자동화된 의사결정(Rights related to automated decision making including profiling)	제4절 제22조

- 정보주체의 권리와 관련된 규정은 컨트롤러가 정보주체의 개인정보를 처리할 때 보다 안전한 기술적·관리적 조치를 취하게 하는 수단으로써 의의가 있다. 또한 이를 통해 기업은 책임성을 강화하고 투명성을 입증하는 데 도움이 된다.



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.



셀프 체크리스트

Self Check List

	예	아니오
• 접근·수정·삭제 등 정보주체가 권리를 행사할 때 법령에서 요구하는 제공 시기 및 방법 등을 준수하여 정보주체에게 정보를 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 이용 약관 및 개인정보처리방침을 쉽게 조회할 수 있도록 정보를 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체로부터 개인정보를 수집하는 경우, 회사가 의무적으로 제공하여야 하는 정보를 개인정보 취득 시점에 즉시 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 제3자가 취득한 개인정보를 제공받을 경우, 의무적으로 제공하여야 하는 정보를 해당 정보주체에게 개별 통지하고 있는가?	<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 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.1 주요 내용

- 정보주체는 자신의 개인정보를 누가, 어떤 목적으로, 무엇을 하는지 등의 정보를 명확하고 간결하게 제공받을 권리를 가진다. 이러한 정보주체의 권리 실현은 GDPR 제5조

제1항(투명성 원칙)과 맞닿아 있으며, 컨트롤러가 정보주체에게 제공하여야 하는 정보와 그 시기 및 방법에 대해 제12조~제14조에 규정하고 있다.

2.2 개인정보의 수집 시 정보 제공 의무

2.2.1 정보 제공의 형식

- 제13조와 제14조는 정보주체의 개인정보를 누가, 어떤 목적으로, 무엇을 하는지 등의 정보를 해당 정보주체에게 모두 “제공”하여야 할 컨트롤러의 의무에 대한 것이다. 이는 컨트롤러가 해당 정보를 정보주체에게 제공하기 위하여 적극적인 조치를 취해야 함을 의미하고 정보주체는 이러한 조항들이 적용되는 정보를 구하거나 웹사이트 또는 앱의 이용약관과 같은 다른 정보들 사이에서 해당 정보를 찾기 위하여 적극적인 조치를 취할 필요가 없어야 함을 의미한다. 이를 위한 방법으로 개인정보처리방침·고지, 푸시 및 폴 알림, 그 밖에 다양한 개인정보 환경에서 정보주체에게 정보를 제공하기 위하여 하드카피를 통한 서면 설명(만화, 인포그래픽, 플로차트), 전화 환경에서의 녹음 정보 제공, 모바일 또는 스마트 기기 환경에서 아이콘, QR코드, 음성 알림정보, 개인 대 개인 환경에서의 구두 설명, CCTV나 드론 녹화 환경에서의 관련 정보가 포함된 게시판 내지 미디어 공지 등을 포함할 수 있다.

2.2.2 제공하여야 하는 정보

제공 정보 내용	정보주체에게 직접 수집하는 경우	정보주체에게 직접 수집하지 않는 경우	WP29 작업반의 해석
컨트롤러와(해당하는 경우) 컨트롤러 대리인의 신원 및 연락처와 DPO의 연락처	○	○	컨트롤러의 신원 확인 및 가급적 컨트롤러와 다양한 형태로 의사교환을 할 수 있게 해 주어야 함
해당 개인정보의 처리 목적 및 처리의 법적 근거	○	○	개인정보 처리 목적을 명시하는 이외에 제6조 내지 제9조에 따라 의존하는 관련 법적 근거를 명시하여야 함
제6조제1항(f)에 의한 처리의 경우 컨트롤러 또는 제3자의 적법한 이익	○	○	정보주체의 이해를 위하여 관련되는 특정한 이해관계를 확인해주어야 함. 모범 관행으로서 LIA 실시하는 경우 그 테스트 정보를 정보주체에게 제공하여야 함
개인정보의 유형	-	○	개인정보가 정보주체로부터 획득되지 않았고 따라서 정보주체는 컨트롤러가 어떠한 유형의 정보를 획득하였는지 알지 못하므로 이 정보는 제14조가 적용되는 경우에 요구됨
개인정보 수령인 또는 수령인의 유형	○	○	수신자는 제3자일 필요 없음. 한편, 공정성의 원칙에 따른 기본 입장은 컨트롤러는 개인정보의 실제 수신자에 대한 정보를 제공하여야 한다는 것이지만, 컨트롤러가 단지 수신자의 범주만을 제공하기로 하는 경우에는 컨트롤러는 이러한 접근법이 왜 공정한지를 입증할 수 있어야 함. 수신자의 범주에 대한 정보는 수신자의 유형, 산업, 부문, 수신자의 위치 등을 명시하는 등 가능한 한 구체적이어야 함
제3국이나 국제기구로 개인 정보를 이전할 예정이라는 사실, 적정성 결정의 유무, 적절하고 적합한 보호수단과 그에 대한 사본 입수 수단	○	○	전송 및 그에 대응하는 메커니즘을 허용하는 관련 GDPR 조항이 명시되어야 함. 가능한 한 사용되는 메커니즘에 대한 링크 또는 정보 획득에 대한 정보도 제공되어야 함. 공정성의 원칙에 따라 정보가 전송되는 모든 제3국을 명시적으로 언급하여야 함

제공 정보 내용	정보주체에게 직접 수집하는 경우	정보주체에게 직접 수집하지 않는 경우	WP29 작업반의 해석
보유기간 또는(여의치 않을 경우) 보유기간 결정을 위하여 적용한 기준	○	○	보유기간은 법적 요건 또는 업계 지침 등의 사항들에 의하여 좌우될 수 있으나 정보주체가 각자의 상황에 따라 특정 정보/목적에 대한 보유기간을 평가할 수 있는 방식으로 진술되어야 함. 컨트롤러가 처리의 합법적 목적을 위해 필요한 기간 동안 개인정보가 보유될 것임을 일반적으로 진술하는 것으로는 충분하지 않음. 적절한 경우, 개인정보 유형 및 처리목적에 따라 각각 보유기간이 규정되어야 함
정보주체에게 인정되는 권리(접근, 수정, 삭제, 처리 제한, 처리에 대한 이의 제기, 이동성)의 유무	○	○	이 정보에는 권리에 무엇이 포함되고 정보주체가 이를 행사하기 위하여 어떤 조치를 취할 수 있는지에 대한 내용이 포함되어야 함
처리가 제6조제1항(a)이나 제9조제2항(a)에 근거한 경우, 철회 이전에 동의를 기반으로 하는 처리의 합법성에 영향을 주지 않고 언제든지 동의를 철회할 수 있는 권리의 유무	○	○	이 정보에는 정보주체가 동의를 제공하는 것만큼 쉽게 철회할 수 있다는 점을 고려하여 동의를 철회할 수 있는 방법이 포함되어야 함
감독기관에 민원을 제기할 수 있는 권리	○	○	이 정보는 제77조에 따라서 정보주체가 자신의 거주지, 근무지, 또는 주장되는 GDPR 위반 장소의 감독기관에 민원을 제기할 권리가 있음을 설명하여야 함
개인정보의 제공이 법률 또는 계약상 요건이나 의무인지 여부 및 정보주체가 개인정보를 제공할 의무가 있는지 여부 및 해당 개인정보를 제공하지 않을 경우 생길 수 있는 영향	○	○	예컨대, 고용의 맥락에서, 기존 또는 잠재적인 피고용인에게 특정 정보의 제공을 요구하는 것은 계약상의 요구사항이 될 수 있다. 온라인 양식에는 필수 필드와 그렇지 않은 필드, 필수 필드를 작성하지 않을 경우의 결과를 분명히 밝혀야 함
프로파일링 등 자동화된 결정의 존재 유무 및 이 경우 관련 로직에 관한 유의미한 정보와 이러한 정보 주체에 대한 처리의 중요성 및 예상되는 결과	○	○	아래 9.2.1(156쪽) 참조

2.2.3 제공 시기

정보주체에게 직접 수집하는 경우	정보주체에게 직접 수집하지 않는 경우
정보를 취득한 때	<ul style="list-style-type: none"> - 개인정보가 처리되는 특정 상황과 관련하여 정보 취득 후 합리적인 기간 내에(최대 1개월) - 개인정보가 정보주체에게 통지 목적으로 이용되는 경우, 늦어도 해당 정보주체에게 최초로 통지한 시점 - 다른 수령인에게 개인정보가 제공될 것으로 예상되는 경우 늦어도 최초로 제공되는 시점

2.3 정보주체의 요청 시 정보제공 의무

2.3.1 제공하여야 하는 정보

- 컨트롤러는 제15조 내지 제22조에 따른 정보주체의 요청에 따라 취해진 조치에 대한 정보를 제공하여야 한다. 컨트롤러는 정보주체의 권리 행사를 용이하게 할 수 있도록 하여야 하고, 컨트롤러는 제11조제2항에 따라 자신이 정보주체를 식별할 위치에 있지 아니하다는 점을 입증하지 않는 한, 제15조 내지 제22조에 따른 정보주체 본인의 권리를 행사하기 위한 요청을 거절해서는 안 된다.

2.3.2 제공 시기

- 컨트롤러는 제15조 내지 22조에 해당하는 정보주체의 요청에 대하여 다음 기준을 준수하여야 한다.
 - ① 요청을 접수한 후 1개월 이내 부당한 지체 없이(without undue delay) 제공한다.
 - ② 요청의 복잡성과 요청 횟수를 고려하여 필요한 경우 2개월 추가 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 1개월 이내에 미 조치 사유, 감독기관에 민원을 제기할 권리, 사법적 구제를 청구할 권리를 정보주체에게 고지하여야 한다.
- 한편, 전달하는 정보 내지 통지와 무관하게, 투명성 의무와 관련한 책임은 개인정보를 수집하는 시점뿐만 아니라 처리 기간 전체에 걸쳐 적용된다. 예컨대 기존 개인정보처리방침(privacy policy notification)의 내용이나 조건을 변경할 때 컨트롤러는 대부분의 정보주체가 실제로 인지할 수 있는 방식으로 이러한 변경이 통지되도록 하여야

하고, 그러한 전달은 직접 마케팅 콘텐츠와 결합 없이 그 변경만을 위하여 적절한 방식으로 통지되어야 한다. 위 통지는 간결하고 이해 가능하고 쉽게 접근할 수 있어야 하며 명확하고 평이한 언어를 사용하여야 한다는 제12조의 요구사항을 충족하여야 한다. 정보주체가 개인정보보호정책·고지의 변경 또는 업데이트를 정기적으로 확인하여야 한다는 취지의 언급을 정책·고지에 포함시키는 것만으로는 불충분하고 또한 이는 제5조의 맥락에서 불공정한 것으로 간주될 수 있다.

2.4 정보 제공 방법

2.4.1 제공 수단(제12조제3항)

- 정보는 문서 또는 전자적 수단을 포함한 그 밖의 방법으로 제공되어야 하고, 정보주체가 요구하는 경우에는 구두로도 제공될 수 있다. 즉, 정보 제공 내지 통지는 기본적으로 ‘문서’로 이루어 져야 하는 것이며, 적절한 경우에는 전자수단을 포함하여 명시되지 않은 다른 ‘기타 수단’의 사용도 허용된다.
 - 단계적 접근법 : 핵심 프라이버시 정보를 짧은 고지로 알려 준 후 추가적인 상세 정보를 단계적으로 제공
 - 대시보드 : 개인정보 이용 현황을 알려 주고 이용 방식의 관리를 허용하는 환경설정 관리 도구
 - 적시 고지 : 개인정보를 수집하는 시점에 프라이버시 정보 전달
 - 아이콘 : 특정 유형의 정보 처리 존재를 알리는 작은 기호
 - 모바일 및 스마트 기기 기능 : 팝업, 음성 알람 및 모바일 기기 제스처
 - 비전자적 수단 : 만화, 인포그래픽, 플로차트 등 활용
- 정보주체의 요청이 전자적 형태로 이루어진 경우 별도의 다른 요청이 없는 한 해당 정보는 가능한 전자적 형태로 제공되어야 한다. 그리고 정보를 제공하기 위하여 선택하는 방식은 특정 상황, 즉 컨트롤러와 정보주체가 상호작용 하는 방식 또는 컨트롤러가 정보 주체의 개인정보를 수집하는 방식에 적절한 것이어야 한다는 점이 매우 중요하다.
- 정보주체에게 구두로 정보가 제공될 수 있으나 이 경우 그들의 신원 정보가 다른 수단에 의하여 증명되어야 한다. ‘구두 정보 제공’은 반드시 개인 대 개인의 방식(직접 또는 전화와 같은 방식)으로 구두 정보가 제공되어야 한다는 것을 의미하는 것은 아니다. 즉, 서면 수단에 더하여 자동화된 구두 정보를 제공할 수도 있다. 예컨대 컨트롤러가 정보주체에게 구두로 정보를 제공하기로 하거나 정보주체가 구두 정보 또는 구두

통지를 요구한다면 컨트롤러는 정보 주체로 하여금 미리 녹음된 메시지를 다시 들을 수 있도록 하여야 한다. 한편, 제13조 및 제14조에서 규정된 일반적인 정보제공은 컨트롤러가 신원을 확인할 수 없는 정보주체에 대하여도 접근 가능성이 보장되어야 하므로, 해당 정보에 대하여는 컨트롤러가 정보 주체의 신원 증명을 요구하지 않고서도 구두 수단을 통하여 제공할 수 있다.

2.4.2 명확하고 쉬운 언어 사용(제12조제1항)

- 투명성 원칙에 따라 모든 통지, 특히 아동을 특정한 정보에 대하여는 평이한 언어를 사용하여, 간결하고, 투명하며, 쉽게 이해할 수 있고, 접근이 용이한 방식으로 제공하기 위한 적절한 조치를 취하여야 한다. 온라인 광고처럼 개인정보의 처리에 다수의 행위자가 관여하게 되고 복잡한 기술이 활용됨에 따라 정보주체가 본인의 개인정보가 누구에 의해 어떤 목적으로 수집되는지 파악하기 어려운 경우와 관련이 있다.
- ‘간결하고 투명한’ 방식의 의미는 정보 피로(information fatigue)를 방지하기 위하여 컨트롤러가 정보 및 통지를 효율적이고 간결하게 제시하여야 한다는 것을 의미하고 또한 계약 내용과 같이 프라이버시와 관련되지 않은 다른 정보와 분명히 구별되어야 함을 의미한다. 예컨대, 온라인에서는 단계별 개인정보처리방침을 통해 정보주체가 특정 이슈를 찾기 위해서 많은 양의 텍스트를 전부 스크롤 할 필요 없이, 즉시 접근하고자 하는 개인정보처리방침의 특정 세션으로 이동하는 것과 같은 간결하고 투명한 방식을 채택할 수 있다.
- ‘쉽게 이해할 수 있다’는 것은 정보주체가 이해할 수 있어야 한다는 점을 의미한다. 이는 컨트롤러가 해당 정보주체를 파악하고 평범한 구성원의 이해수준을 확인할 필요가 있음을 의미한다. 또한 목표 정보주체와 실제 정보주체의 이해수준이 다를 수 있으므로 관리자는 정보·통지가 여전히 실제 이용자(특히 아동으로 구성된 경우)에 맞추어져 있는지를 정기적으로 확인하고 조정하여야 한다.
- ‘쉽게 접근할 수 있다’의 의미는 정보주체가 정보를 찾아다닐 필요 없이 해당 정보를 어디서 접근할 수 있는지 바로 알 수 있어야 한다는 점을 의미한다. 예컨대, 정보를 직접 제공하거나, 링크를 제공하거나, 분명한 안내 표시를 하거나, 자연어 질문(사람이 읽을 수 있는)의 답변 방식을 제공하여야 한다. 웹사이트를 유지하는 조직은 웹사이트에 개인정보 보호정책·고지를 게시할 수 있고, 그 링크는 웹사이트의 각 페이지에서 일반적으로 사용되는 용어 아래에 분명하게 눈에 띄는 방식으로 배치되어야 한다. 웹페이지에서 텍스트나 링크가 덜 뚜렷하거나 찾기 어렵게 만드는 배치, 색상 구성은 쉽게 접

근할 수 있는 것으로 평가되지 않는다. 앱의 경우, 다운로드 전에 온라인 스토어에서 필요한 정보를 이용할 수 있어야 하고, 일단 앱을 설치한 후에 정보 확인에 필요한 탭의 수가 2회를 넘어서는 안 된다. 이는 앱에서 흔히 사용되는 메뉴 기능에 개인정보·정보보호 옵션이 포함되어야 한다는 점을 의미한다. 이와 함께, WP29는 온라인 맥락에서 개인정보의 수집 시점에 개인정보처리방침에 대한 링크를 제공하거나 개인정보를 수집하는 위치와 동일한 페이지에 해당 정보를 제공할 것을 권고하고 있다.

- ‘명확하게 쉬운 언어’의 의미는 복잡한 문장과 언어구조를 피하고 가능한 간단한 방식으로 정보를 제공하여야 한다는 것을 의미한다. 예컨대, 처리 목적과 관련하여 ‘새로운 서비스 개발’, ‘연구목적’, ‘맞춤 서비스 제공’은 그 목적이 충분히 명확하지 않다고 해석될 수 있다. 또한 컨트롤러가 하나 이상의 다른 언어를 사용하는 정보주체를 대상으로 하는 경우 해당 언어로 된 번역을 제공하여야 한다.
- 아동에게 특별한 보호수단이 필요하다는 점을 고려할 때 아동을 대상으로 한 정보처리 경우 모든 통지 및 의사표시는 해당 아동이 쉽게 이해할 수 있는 명확하고 쉬운 언어가 이용되어야 한다. 즉, 아동에게 어울리고 공감이가 어휘, 어조, 문체를 사용하여 정보를 수신하는 아동이 메시지 및 정보가 자신을 대상으로 한 것임을 알 수 있도록 해야 한다. 또한 컨트롤러가 그들의 상품·서비스가 장애인 또는 정보에 접근하는데 어려움이 있는 사람들 및 다른 취약 계층에 의해 사용된다는 점을 인지하는 경우, 컨트롤러는 해당 정보주체와 관련된 투명성 의무를 준수하는 방법을 평가할 때 그들의 취약성을 고려하여야 한다.

2.4.3 무상 제공(제12조제5항)

- 제13조 및 제14조에 따라 제공되는 정보와 제15조부터 제22조까지와 제34조에 따라 취해진 모든 통지와 조치는 무료로 제공되어야 한다. 컨트롤러는 제13조 및 제14조에 따른 정보제공 또는 제15조 내지 제22조, 제34조에 따라 취해진 통지 및 조치에 대하여 정보주체에게 요금을 청구할 수 없다. 이는 투명성 요구사항에 따라 제공되는 정보가 재정적 거래, 예컨대 상품 또는 서비스에 대한 구입 또는 지불을 조건으로 할 수 없음을 의미한다. 예컨대, 구매와 관련하여 정보주체의 개인정보가 수집되는 경우 제13조에 따라 제공해야 하는 정보는 거래가 마무리된 후가 아니라 결제가 이루어지기 전, 그리고 정보가 수집되는 시점에 제공되어야 한다. 또한 정보주체에게 무료 서비스가 제공되는 경우 제13조제1항이 “개인정보를 획득하는 시점”에 정보를 제공할 것을 요구하는 점을 고려하여 제13조의 정보는 등록 후가 아닌 그 전에 제공되어야 한다.

- 정보주체의 요구가 명백하게 근거가 없거나 과도한 경우, 특히 요청이 반복적인 경우 컨트롤러는 (i) 정보 내지 통지를 제공하거나 요청된 조치를 취하는 행정적 비용을 고려하여 합리적인 수수료를 부과하거나, (ii) 요청에 따른 조치의 거부를 할 수 있다. 다만, 요청이 명백하게 근거가 없거나 과도하다는 점을 입증할 책임은 컨트롤러에게 있다.

2.4.4 가독성이 높은 표준화된 아이콘의 제공(제12조제7항, 제8항)

- 제13조 및 제14조에 의하여 제공되는 정보는 쉽게 눈에 띄고, 이해할 수 있으며, 분명하게 가독할 수 있는 방식으로, 의도하는 처리 내용에 대한 주요한 개요(overview)를 설명할 수 있도록 표준화된 아이콘과 함께 제공되어야 한다. 아이콘은 방대한 양의 서면 정보를 정보주체에게 제시할 필요성을 줄이고 정보 주체를 위한 투명성을 제고하기 위하여 제안된 것이다. 아이콘의 사용은 정보의 제공과 함께 이루어지는 것이므로 아이콘의 사용이 정보주체에 대한 권리 행사에 필요한 정보를 대체해서는 안 되고, 제13조 및 제14조에 따른 컨트롤러의 의무준수에 대한 대체물로 사용되어서도 안 된다.
- 아이콘이 전자적으로 제공되는 경우 컴퓨터에 의한 판독이 가능(machine-readable)하여야 한다. 컴퓨터에 의한 판독이 가능한 형식은 개방 또는 독점적 형식일 수 있고, 공식 표준일 수도 아닐 수도 있다. 정보를 추출할 수 없거나 또는 쉽게 추출할 수 없기에 자동처리가 제한되는 파일 형식으로 인코딩된 문서는 컴퓨터에 의한 판독이 가능한 형식으로 간주할 수 없다. 예컨대, 아이콘이 물리적 문서, IoT 장치 또는 IoT 장치의 포장, 공공장소의 Wi-Fi 추적에 대한 고지, QR 코드, CCTV 고지에 제시되는 등 아이콘이 전자적으로 제시되지 않는 상황도 있을 수 있다.
- 유럽집행위원회는 제92조에 따라 아이콘에 의하여 제시될 정보와 표준화된 아이콘을 제공하는 절차를 결정할 수 있다.

2.5 추가 처리

- 컨트롤러가 당초 개인정보 수집 목적 이외의 목적으로 개인정보를 추가 처리(further processing)할 예정인 경우 컨트롤러는 해당 처리 이전에 정보주체에게 관련된 정보를 제공하여야 한다.

- 정보주체가 이미 관련 정보를 보유하고 있는 경우 수집 시 정보의 제공에 대한 사항(제13조제1항 내지 제3항, 제14조제1항 내지 제4항)은 적용되지 않는다. 책임성의 원칙에 따라서 본 적용 제외를 주장하고자 할 경우 컨트롤러는 정보주체가 어떤 정보를 이미 보유하고 있고, 이를 언제 어떻게 수신하였으며 이후 그 정보에 대하여 업데이트가 필요한 어떠한 변경도 이루어지지 않았다는 것을 입증하여야 한다. 또한 정보주체가 이전에 제13조에서 명시된 정보의 목록에서 특정 범주를 제공받았다고 하더라도 컨트롤러는 정보주체가 제13조제1항 및 제2항에 열거된 정보의 완전한 세트를 보유할 수 있도록 그 정보를 보충하여야 할 의무를 부담한다.
- 정보주체 이외의 자로부터 수집된 개인정보 및 그 처리 활동이 아래의 조건에 해당하는 경우에는 적용의 제외가 추가적으로 인정 된다.
 - 제89조제1항에 따라 공익상 기록보관, 과학이나 역사 연구 목적, 통계목적으로의 처리에 대해, 해당 정보의 제공이 불가능하거나 과도한 노력이 수반되어야 하는 경우, 또는 제14조제1항에 규정된 의무가 불가능하다고 생각되거나 관련 처리의 목적 달성을 심각하게 저해하는 경우.(단, 이 경우 컨트롤러는 해당 정보의 공개 등 정보주체의 권리와 자유, 적법한 이익의 보호를 위한 적절한 조치를 취하여야 한다.)
 - 컨트롤러에게 적용되고, 정보주체의 적법한 이익을 보호하기 위하여 적절한 조치를 규정한 유럽연합과 회원국 법률에서 그 취득과 제공에 대하여 명백하게 규정하고 있는 경우
 - 개인정보가 유럽연합 또는 회원국 법률에 의해 규제되는 직무상 비밀유지의무에 따라 비밀로 유지되어야 하는 경우

⇒ 사례

프랑스 개인정보보호위원회(CNIL)는 2019. 01. 21. 구글이 개인정보 처리방침에 투명하고 이해하기 쉬운 방식으로 관련정보를 게시하지 않은 행위, 광고 개인화를 목적으로 하는 개인정보 수집에 대한 동의를 구체적이고 명료하게 받지 않은 행위 등에 대하여 5,000만 유로의 과징금을 부과하였다.

- 프랑스 개인정보보호위원회가 구글에 대하여 과징금을 부과한 구체적인 이유는 GDPR이 규정하는 투명성 원칙 및 동의 요건을 위반했다는 것이다. 투명성 원칙 위반으로 판단한 이유로는 개인정보 처리 목적, 보유기간, 맞춤형 광고에 사용되는 정보의 유형과 같은 필수 정보들이 과도하게 분산되어 있고 전체 정보를 얻기 위해서는 링크와 버튼을 다수 사용하여야 하며, 관련 정보들은 심지어 5, 6단계를 거쳐야만 접근할 수 있었다는 점이다. 그리고 개인정보 처리 목적이 지나치게 일반적(generic)이고 불명확(vague)하며, 여러 목적을 위해 처리되는 개인정보의 유형 역시 마찬가지라는 점이다. 또한 커뮤니케이션 정보가 명확하지 않아서 이용자들로서는 처리의 법적 근거가 '적법한 이익'이 아닌 '동의'라는 점을 이해하기도 어려우며, 일부 개인정보에 대하여는 그 보유기간에 대한 정보가 제공되고 있지 않다는 점이다.
- 동의 요건 위반으로 판단한 이유는, 앞서 본 바와 같이 동의를 위하여 제공되는 정보가 지나치게 흩어져 있고 이용자가 이해하기 어렵다는 점이다. 예컨대, “맞춤형 광고”와 관련하여, 그 개인정보의 처리가 이루어지는 서비스, 웹사이트, 앱의 숫자뿐만 아니라 처리되고 결합되는 데이터의 양에 대하여도 이해하기 어렵다. 또한, 이용자는 ‘설정’ 기능을 통하여 “맞춤형 광고”에 대한 옵션을 변경할 수 있으나, 개인화 광고 기능이 사전 체크(pre-ticked) 되어 있는 점에서 그 동의가 명백하다고 할 수 없다. 그리고 계정 생성 시 약관 동의와 개인정보 처리 동의 박스를 클릭하여 전체 처리 목적을 일괄하여 동의하도록 되어 있는데, 이는 특정(specific)하여 동의를 받도록 한 GDPR에도 부합하지 않는다는 것이다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제12조(정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식) ■ 제13조 및 제14조(정보를 제공받을 권리) ■ 전문 제58항~제62항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)



정보주체의 접근권

(Right of access by the data subject)



Point

- 정보주체의 접근권에 대한 개념과 접근 가능한 정보의 종류를 이해할 수 있다.
- 접근권 요청에 따른 조치 사항과 제공 방법 및 이행 시기를 이해할 수 있다.



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체가 본인과 관련된 개인정보 처리에 대하여 접근을 요청하는 경우 이를 처리하는 메커니즘(절차 및 체계)과 양식을 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 본인과 관련된 개인정보 처리에 대하여 접근을 요청하는 경우, 처리 목적, 개인정보 유형 등의 내용 및 조치 사항에 대하여 정보를 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

3.1 주요 내용

- 정보주체는 본인과 관련된 개인정보의 처리 여부에 관련하여 컨트롤러로부터 확인을 받을 수 있는 권리를 가진다. 컨트롤러는 정보주체의 접근 요구가 있을 경우에 아래의 정보에 대하여 접근(access)할 수 있도록 조치하여야 한다(제15조제1항).

- ① 처리 목적
- ② 관련된 개인정보의 유형(category)³¹
- ③ 개인정보를 제공받았거나 제공받을 수령인 또는 수령인의 범위

31 '유형'(category)에 대한 접근권이 부여된다는 의미는 처리되는 관련 개인정보의 전부를 접근할 수 있다는 의미가 아니며 그 유형에 대한 접근 청구권을 가진다는 의미이다.

- ④ (가능하다면) 개인정보의 예상 보유기간 또는(가능하지 않다면) 해당 기간을 결정하기 위하여 이용되는 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 가능한 정보
- ⑧ GDPR 제22조제1항, 제4항에 규정된 프로파일링 등 자동화된 의사결정의 유무와 관련 로직에 대한 유의미한 정보, 이러한 처리가 정보주체에 미치는 유의성과 예상되는 결과

3.2. 국외 이전 시

- 개인정보가 제3국이나 국제기구에 이전되는 경우, 정보주체는 GDPR 제46조에 따라 적절한 안전조치에 대한 정보를 고지 받을 권리를 가진다(제15조제2항).

3.3 접근 요구 시 조치 사항

3.3.1 사본의 무상 제공

- 컨트롤러는 정보주체의 접근 요구에 따라 처리가 진행 중인 개인정보의 사본을 제공하여야 한다. 그 제공은 원칙적으로 무상이어야 한다. 다만, 정보주체의 요구에 명백하게 근거가 없거나 반복적인 요구 등 과도하다면 합리적인 비용을 부과하거나 이를 거부할 수 있다(제12조제5항). 또한 정보주체가 추가적인 사본 제공을 요구하는 경우 컨트롤러는 행정적 비용에 근거한 합리적인 비용 청구가 가능하다.

3.3.2 제공 방법

- 컨트롤러는 정보주체가 자신의 개인정보에 대한 접근권을 쉽게 행사할 수 있도록 관련 절차와 양식(form)을 제공하여야 한다. 정보주체의 요구가 전자적 형태로 이루어졌다면, 컨트롤러는 정보주체가 달리 요구하지 않는 한 가능한 전자적 형태로 제공하여야 한다. 또한, 컨트롤러는 가능한 한 정보주체가 안전한 시스템을 통하여 자신의 개인정보에 직접 원격으로 접속할 수 있도록 하여야 한다. 정보주체의 이러한 권리는 영업비밀,

지식재산권, 저작권 등을 포함하여 다른 사람의 권리와 자유를 침해하여서는 안 되지만(제15조제4항), 그로 인하여 정보주체의 권리가 전체적으로 거부되어서도 안 된다.

- 컨트롤러는 접근을 요청한 정보주체의 신원확인을 위하여, 특히 온라인 서비스의 제공 및 온라인 식별과 관련하여 합리적인 모든 수단을 활용하여야 한다. 그러나 컨트롤러는 잠재적 요청(potential request)의 응대라는 유일한 목적만으로 개인정보를 보유해서는 안 된다(전문 제64항).

3.3.3 이행 시기

- 컨트롤러는 ‘부당한 지체 없이(without undue delay)’ 그리고 ‘늦어도 1개월 이내’에 정보주체의 요청에 따라야 한다.
요청이 복잡하거나 여러 건의 요구를 처리할 경우에는 이행 기간을 2개월 추가 연장할 수 있다. 그러나 이 경우에도 해당 요구를 접수한 날로부터 1개월 이내에 해당 정보주체에게 연장이 필요한 이유를 통지하여야 한다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)■ 제15조(정보주체의 접근권)■ 전문 제59항, 제63항, 제64항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제35조(개인정보의 열람)■ 제38조(권리 행사의 방법 및 절차)



정정권 (Right to rectification)



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• 부당한 지체 없이 그리고 정정 요청 수령일로부터 1개월 이내에 정정 요청에 응답하기 위한 확실한 절차를 갖추고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 특히 정보주체가 본인과 관련된 개인정보 처리에 대하여 정정권을 요청하는 경우, 이를 처리하는 절차와 양식을 제공하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보를 정정하거나 입력·보충할 적절한 시스템을 갖추고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 제3자와 공유하는 정보를 수정하는 경우에 해당 제3자에게 알리기 위한 절차를 갖추고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.1 주요 내용

- 개인정보의 정확성 원칙(제5조(1)(d))은 정보주체를 높은 수준으로 보호하기 위해서 필수적인 것이다.³² 정보주체는 본인에 관한 개인정보에 대하여 정확하지 않은 부분을 수정하도록 컨트롤러에게 요구할 수 있다(제16조). 또한 정보주체는 처리 목적을 고려

32 ECtHR, Ciubotaru v. Moldova, No. 27138/04, 2010. 04. 27., pp.51~59.

하여 컨트롤러에게 추가 정보를 제공함으로써 불완전한 정보를 보완할 수 있는 권리를 가진다.

- 이름의 철자나, 주소의 변경, 전화번호의 변경 등은 단순한 요구만으로도 정정이 가능하다. 그러나 정보주체의 법적인 본인 확인 용도이거나 법률 문서의 송달을 위한 거주지 주소의 변경과 같은 경우에는 단순한 정정 요구만으로는 부족하고, 컨트롤러는 기존 정보의 부정확성을 확인하기 위한 증거를 요구할 수 있다.³³ 그러나, 그러한 요구가 정보주체에 대한 불합리한 수준의 입증 부담을 지게 하여서는 안 된다.

4.2 정정 요구 시 조치 사항

- 컨트롤러는 정보주체의 정정 요구가 있으면 부당한 지체 없이(without undue delay) 다음과 같이 필요한 조치를 하여야 한다.
 - ① 정정을 위한 조치는 정정 요구를 받은 시점으로부터 1개월 이내에 이행하여야 한다. 다만 정정 요구가 복잡한 경우 2개월 추가 연장이 가능하다(제12조제3항).
 - ② 정정 요구에 따른 조치를 취하지 않은 경우 정보주체에게 그 이유 및 감독기구에 민원을 제기할 수 있고 사법적 구제를 청구할 수 있음을 알려 주어야 한다(제12조제4항).
 - ③ 개인정보를 수령인에게 공개·제공하였다면 가능한 한 그 수령인에게 정정에 대하여 통지하여야 한다(제19조). 또한 컨트롤러는 정보주체가 요구하는 경우 그 정보의 수령인에 대하여도 정보주체에게 통지하여야 한다.

4.3 정정 요구를 거절할 수 있는 사유

- 컨트롤러는 정보주체의 정정 요구가 있다고 하더라도 (1) 명백히 사실무근인 경우이거나 (2) 과도한 경우에는 해당 정정 요구를 거절할 수 있다. 개인이 명백하게 정정권을 행사할 의사가 없는 경우이거나 그 요구가 의도적으로 악의적이고 혼란을 야기하는 것 외에 어떠한 실제 목적도 없이 컨트롤러를 괴롭히려고 정정권을 행사하는 경우에는 명백히 사실무근인 것으로 판단할 수 있다. 이전의 정정 요구와 본질적으로 동일한 내용을 반복하거나 다른 요구와 중복되는 경우에는 해당 정정 요구는 과도한 것으로

33 FRA, Handbook, pp.220.

로 판단할 수 있다. 그러나 과도함의 판단은 특정 상황에 따라 달라질 수 있으며, 정보주체가 동일한 쟁점에 대하여 요청하거나 이전에 제출된 요구였다는 이유만으로는 반드시 과도하다고 판단하기는 어렵다. 특히, 정정 요구가 완전히 다른 데이터 세트와 관련된 경우에는 동일한 정보주체의 중복 요구라고 하더라도 과도하지 않다고 판단할 여지가 있다.

⇒ 사례

정보주체는 자신의 정보가 부정확하다고 판단하여 컨트롤러에게 반복적으로 정정 요청을 했다. 그러나 컨트롤러가 기존 요청에 대해 확인해보니 해당 정보가 정확했고, 이를 정보주체에게 통지했다. 이후 정보주체는 별다른 근거 없이 컨트롤러에게 지속적으로 관련 정보의 정정을 요청했다. 이 경우 컨트롤러는 정보주체의 요구가 명백히 사실무근이고, 관련 내용에 대해 이미 정보주체에게 통지하였으므로 정보주체의 가장 최근의 정정 요구에 대하여는 거절할 수 있다.

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)

한국 개인정보보호법 관련 규정

- 제36조(개인정보의 정정·삭제)



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.



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체가 본인과 관련된 개인정보에 대하여 삭제를 요청하는 경우, 법적 근거에 따라 요청 사항을 조치하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

5.1 주요 내용

- 정보주체는 컨트롤러에게 본인에 관한 개인정보의 삭제를 요구할 권리를 가진다(제17 조제1항). 이 권리는 정보주체가 원하는 경우 자신에 관한 개인정보를 삭제하도록 함으로써 개인정보의 처리가 더 이상 이루어지지 않도록 하기 위한 권리이다. 특히 GDPR에서는 해당 개인정보가 제3자에게 공개된 경우 해당 제3자들에 대하여도 일정한 사항을 알리고 합리적 조치를 취하도록 할 의무를 부과하고 있다.
- 스페인 변호사 마리오 곤잘레스는 1998년에 있었던 자신의 파산 사건과 관련한 신문 기사가 구글 검색엔진을 통하여 검색되는 것이 사생활의 침해에 해당한다는 이유로 2010년 스페인 법원에 구글 및 해당 신문사를 상대로 기사 삭제 소송을 제기하였고 스페인 법원은 해당 사안과 관련한 법률적 판단을 유럽사법재판소에 의뢰하게 된다. 삭제권은 2014년 5월 13일, EU 개인정보보호지침을 근거로 유럽사법재판소가 구글에

대하여 관련 링크를 삭제하여야 한다고 판시³⁴함으로써 구체화되었으며³⁵ 그 내용이 GDPR에 반영되었다.

※ 삭제권은 '잊힐 권리'라고도 하는데, GDPR에서 명시하는 삭제권이 절대적인 '잊힐 권리'를 제공하는 것은 아니다(전문 제65항~제66항).³⁶

- 컨트롤러는 다음 중 하나에 해당할 경우 부당한 지체 없이(without undue delay) 개인정보를 삭제할 의무를 부담한다.
 - ① 개인정보가 수집 목적 또는 다른 방식으로 처리되는 목적에 더 이상 필요하지 않은 경우
 - ② 정보주체가 동의를 철회하고 해당 처리에 대한 다른 법적 근거가 없는 경우
 - ③ 정보주체가 제21조제1항(국가 안보·국방·공공안보·범죄예방)에 따라서 처리에 반대하고 관련 처리에 대하여 우선하는 정당한 사유가 없는 경우, 또는 제21조제2항에 따라서 직접 마케팅을 위한 처리에 반대하는 경우
 - ④ 개인정보가 불법적으로 처리된 경우(GDPR 위반 등)
 - ⑤ 정보처리자에 적용되는 유럽연합 내지 회원국 법률에 따른 법적 의무 준수를 위하여 삭제되어야 하는 경우
 - ⑥ 아동에게 직접 제공되는 정보 사회 서비스와 관련하여 개인정보가 수집된 경우 개인정보의 처리가 합법적이라는 점에 대한 입증 책임은 컨트롤러에게 있다. 책임의 원칙에 따라 컨트롤러는 언제라도 개인정보 처리에 정당한 근거가 있음을 보여줄 수 있어야 한다.
- 개인정보를 수령인에게 공개·제공하였다면 가능한 수령인에게 그 삭제에 대하여 통지하여야 한다(제19조). 또한 컨트롤러는 정보주체가 요구하는 경우 그 정보의 수령인에 대하여도 정보주체에게 통지하여야 한다.

34 CJEU C-131/12, Google Spain SL, Google Inc. v. Agencia Espanola de Protección de Datos(AEPD), Mario Costeja González [GC], 2014, 05. 13.

35 제29조 작업반은 2014. 11. 26. 위 판시에 따른 가이드라인을 채택하였다. 제29조 작업반, Guidelines on the implementation of the CJEU judgement on "Google Spain and Inc. v. Agencia Espanola de Protección de Datos(AEPD), Mario Costeja González" C-131/12, 2014. 11. 26.

36 CJEU, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 9 March 2017에서 CJEU는 10년보다 더 이전에 파산된 회사에 자신이 운영자로 기록된 회사 등록부의 관련 기록 삭제를 요구한 신청인의 청구에 대하여 신청인의 개인정보보호에 관련된 권리와 그 정보 열람에 대한 공중의 이익을 비교衡量하였고, 시간의 경과에도 불구하고 해당 정보가 여전히 공중에 의하여 열람될 필요도 있기에, 본건에 있어서 EU의 개인정보보호 지침이 신청인에게 해당 개인정보의 삭제를 요구할 권리를 보장하는 것은 아니라고 판시하였다.

5.2 개인정보가 공개된 경우

- 컨트롤러가 개인정보를 공개(made public)하였고 제17조제1항에 따라 삭제 의무를 부담하는 경우, 컨트롤러는 가능한 기술과 비용을 고려하여 해당 개인정보를 처리하고 있는 다른 컨트롤러들에게 정보주체가 그들에 의한 해당 개인정보에 대한 링크, 사본, 복제물의 삭제를 요청하였음을 알리기 위하여 기술적 조치 등 합리적 조치를 취하여야 한다. 해당 조치는 가용할만한 기술 및 수단을 고려한 것이어야 한다(전문 제66항). 이는 온라인 환경에서 정보주체에게 부여된 ‘잊힐 권리’를 강화하기 위한 것이다.

5.3 삭제 거부 가능한 경우

- 컨트롤러는 다음 중 하나에 해당될 경우에는 삭제 요구를 거부할 수 있다(제17조제3항).
 - ① 표현 및 정보의 자유에 관한 권리 행사를 위한 경우
 - ② 유럽연합 또는 회원국 법률에 따른 법적 의무를 준수 내지 공익을 위한 직무 수행을 위한 경우, 컨트롤러에게 부여된 공적 권한의 행사를 위한 경우
 - ③ 공중 보건 분야의 공익을 위한 경우
 - ④ 공익을 위한 기록 보존, 과학적·역사적 연구 또는 통계 목적을 위한 것인 경우로서 삭제권의 행사가 불가능하다고 생각되거나 삭제권의 행사로 해당 처리의 목적 달성을 심각하게 저해할 가능성이 있는 경우
 - ⑤ 법적 청구권의 입증(establishment), 행사나 방어를 위한 경우

5.4. 최근 사례

- 프랑스 개인정보보호위원회(CNIL)는 구글이 제기한 10만 유로의 벌금에 대한 불복 사건에서 유럽사법재판소(European Court of Justice)에 삭제권의 적용 범위를 확인하기 위한 판단을 요청하였다. 이 사건과 관련하여 유럽사법재판소는 2019년 9월 24일에 개인정보보호 지침 및 GDPR에 따른 개인정보의 삭제권은 EU 회원국 내에 모두 미치지만 EU 외의 국가에까지는 미치지 아니하므로, 검색 엔진 운영자가 관련 규정에 따라 검색 결과에 대한 링크를 삭제하도록 요구를 받았을 때, 모든 검색 엔진에서 해당 링크를 삭제하여야 할 의무가 부여되는 것은 아니고 회원국 내에 상응하는 검색 엔진 버전에 대하여 링크를 삭제하거나 EU 회원국 내의 하나에서 검색을 수행하는 인터넷 이용자들이 해당 검색 결과를 얻기 어렵게 하는 조치를 취하여야 한다는 의미라고 판단하였다(C-507/17).

GDPR 관련 규정

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

한국 개인정보보호법 관련 규정

- 제36조(개인정보의 정정·삭제)



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 있는가?



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체가 본인과 관련된 개인정보 처리 제한을 요청하는 경우, 법적 근거에 따라 개인정보 처리를 제한하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

6.1 주요 내용

- 정보주체는 자신에 관한 개인정보의 처리를 차단하거나 제한할 권리를 갖는다(제18조 제1항). 개인정보 처리가 제한되면 컨트롤러는 그 정보를 보유만 할 수 있고 이용, 제공 등의 처리는 제한된다. 정보주체의 처리 제한권은 개인정보의 정확성, 처리의 합법성 등에 대하여 다툼이 있거나 소송 수행 등을 위하여 보존의 필요성이 있는 경우에 이용을 제한하되 삭제를 보류할 수 있도록 요구할 수 있는 권리이다.
다음 중 하나에 해당할 경우에 컨트롤러는 정보주체의 개인정보 처리 제한 요구를 이행하여야 한다.
 - ① 정보주체가 개인정보의 정확성에 이의를 제기한 경우, 개인정보의 정확성을 입증할 때까지 처리를 제한

- ② 정보의 처리가 불법적으로 이루어지고, 정보주체가 개인정보의 삭제에 반대하면서 대신에 그 개인정보의 이용 제한을 요청한 경우
 - ③ 더 이상 개인정보가 필요하지 않지만, 정보주체가 법적 청구권의 입증(establishment), 행사나 방어를 위하여 그 정보를 요구한 경우
 - ④ 정보주체가 제21조제1항에 따라 처리에 반대한 경우, 컨트롤러의 정당한 근거가 정보주체의 정당한 근거에 우선하는지 여부가 확인될 때까지 그 처리를 제한
 - 개인정보를 수령인에게 공개·제공하였다면 가능한 수령인에게 해당 처리 제한에 대하여 통지하여야 한다(제19조). 또한 컨트롤러는 정보주체가 요구하는 경우 정보의 수령인에 대하여도 정보주체에게 통지하여야 한다.
- 개인정보 처리 제한의 방법은 다음과 같다(전문 제67항)
- ① 선택된 정보를 임시로 다른 처리시스템으로 이전
 - ② 선별된 개인정보를 이용하지 못하도록 조치 또는 공개적으로 접근하지 못하도록 하거나 공개된 개인정보를 웹사이트에서 임시로 제거
 - 또한 자동 파일링시스템에서의 개인정보 처리 제한은 원칙적으로 개인정보가 추가 처리, 변경되지 않도록 하는 기술적 수단 적용이 필요하고, 개인정보 처리가 제한된다는 사실이 해당 시스템에서 명백하게 표시되어야 한다(전문 제67항).

6.2 처리가 가능한 경우

- 제18조제1항에 따라 개인정보 처리 제한권이 인정되는 경우에도 불구하고 다음 중 하나에 해당되는 경우에는 처리할 수 있다.
 - ① 정보주체의 동의가 있는 경우
 - ② 법적 청구권의 입증(establishment)이나 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(제18조제3항).

GDPR 관련 규정	<ul style="list-style-type: none">■ 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 제67항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제37조(개인정보의 처리 정지)■ 제38조(권리 행사의 방법 및 절차)



개인정보 이동권 (Right to data portability)



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체가 본인과 관련된 개인정보의 이동을 요청하는 경우, 법적 근거에 따라 이동권(회사와 온라인 서비스 간 등) 요청을 조치하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

7.1 주요 내용

- 개인정보 이동권(제20조)은 정보주체의 개인정보를 다른 컨트롤러에게 전송할 수 있게 해줌으로써 정보주체에게 자신과 관련한 개인정보에 대하여 더 많은 통제력을 부여하고 또한 EU 내에서 개인정보의 자유로운 흐름을 지원하며 컨트롤러들 간의 경쟁을 촉진하며 디지털 단일시장(digital single market) 전략 맥락에서 새로운 서비스 개발을 유도하기 위하여 마련된 것이다.³⁷⁾
- 개인정보 이동권은 처리한 개인정보를 받을 수 있는 권리와 한 컨트롤러로부터 다른 컨트롤러에게 개인정보를 전송할 수 있는 두 가지의 내용으로 구성된다.

37 제29조 작업반, Guidelines on the right to data portability, 2017. 04. 05., p.3.

- ① 정보주체가 컨트롤러에게 제공한 자신에 관한 개인정보를 체계적으로 구성되고, 일반적으로 사용되며, 기계 판독이 가능한 형식으로 제공받을 권리
- ② 기술적으로 가능한 경우 그 정보를 다른 컨트롤러에게 직접 이전할 것을 요구할 수 있는 권리
- 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

⇒ 사례

한 정보주체는 온라인 서점에서 구입한 도서 목록 또는 음악 스트리밍 서비스의 플레이 리스트를 추출하는데 관심이 있을 수 있다. 또 다른 정보주체는 결혼식 초대 목록을 만들기 위하여 웹 메일 어플리케이션에서 자신의 연락처 목록을 추출하기를 원할 수도 있으며, 혹은 각각 다른 고객 카드를 이용하여 구매에 관한 정보를 얻고자 할 수도 있다. 이러한 경우에 정보주체는 개인정보 이동권을 행사할 수 있다.

- 개인정보의 처리가 동의 또는 계약 이외의 법적 사유를 근거로 하는 경우에는 이 권리는 적용되지 아니한다. 따라서 공공의 이익을 위하여 컨트롤러가 처리하는 개인정보에 대하여는 이동권이 인정되지 아니한다.
- 그 대상이 되는 개인정보는 자동화된 수단에 의하여 처리되는 개인정보에 한정된다(전문 제68항). 구체적으로 ‘정보주체와 관련된 개인정보’이어야 하므로 ‘익명’정보나 ‘정보주체와 관련이 없는 정보’는 이 유형에 포함되지 아니하고, ‘정보주체에 분명하게 연결될 수 있는 가명 개인정보’는 이에 포함된다. 또한 정보주체가 제공한 개인정보이어야 하는데, 그 범위에는 정보주체가 적극적으로 제공한 정보(예컨대, 회원 가입 시 입력한 이메일 주소, 사용자 이름, 연령 등), 관찰된 개인정보(개인의 검색 이력, 트래픽 정보, 위치 개인정보 등)를 포함하며, 정보주체가 제공한 개인정보를 기반으로 컨트롤러에 의하여 생성된 정보, 즉 추론 정보(inferred data, 예컨대 프로파일링에 의하여 창출된 개인정보)나 파생정보(derived data)는 정보주체가 제공한 정보에 해당하지 않는다. 자동화된 수단에 의하여 처리되는 개인정보에 한정됨으로 종이파일은 제외된다.

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 제공한다.(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 처리시스템을 채택하거나 유지하도록 하는 의무가 부과되는 것은 아니다.

- 컨트롤러는 한 개인이 개인정보의 이동을 요청하는 경우 정보주체의 신원을 명확하게 확인할 수 있는 인증 절차를 시행하여야 한다.

7.2.2 이행 시기

- 컨트롤러는 ‘부당한 지체 없이(without undue delay)’ 그리고 ‘늦어도 1개월 이내’에 정보주체의 요청에 따라야 한다.

요청이 복잡하거나 여러 건의 요구를 처리할 경우에는 이행 기간을 2개월 추가 연장할 수 있다. 그러나 이 경우에도 해당 요구를 접수한 날로부터 1개월 이내에 해당 정보주체에게 연장이 필요한 사유를 통지하여야 한다.

요구에 대한 조치를 취하지 않을 경우 부당한 지체 없이(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

- 개인정보 이동권의 행사는 삭제권(제17조)을 침해하여서는 안 된다. 이동권 행사가 정보주체가 제공한 본인의 개인정보 삭제를 의미하지는 않는다. 또한 이동권은 공익상의 업무를 수행하기 위하여 또는 컨트롤러에게 부여된 공적 권한의 행사를 위하여 필요한 처리에는 적용되지 않는다. 개인정보 이동권으로 인해 지적재산권이나 영업 비밀 등 다른 사람의 권리가 침해되는 경우에는 이동권에 대한 의무가 적용되지 않는다.

- 컨트롤러는 이동 가능한 개인정보를 인가받지 않은 또는 불법적인 처리와 예상하지 못한 손실, 파괴 또는 손상으로부터 보호하기 위하여 추가 인증, 암호화 등 개인정보에 적절한 보안이 적용되도록 보장하여야 한다. 또한 관련된 제3자에게 불리한 영향을 미치는 경우를 막기 위하여 개인정보를 제공받은 컨트롤러는 다른 정보주체의 개인정보를 제외시킬 수 있는 수단을 시행하여야 하고, 관련된 다른 정보주체에 대한 동의 메커니즘을 시행하여야 한다.
- 정보주체의 개인정보 이동권 행사에 응하는 컨트롤러는 그에 따라 개인정보를 제공받은 정보주체 또는 개인정보를 받은 다른 수령자의 처리행위에 책임을 지지 않는다. 개인정보 이동권으로 인하여 컨트롤러가 필요한 기간 이상으로 혹은 특정한 보유기간을 넘어서 개인정보를 보유할 의무를 부담하지는 않는다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제12조(정보주체의 권리를 행사하기 위한 투명한 정보, 통지 및 형식)■ 제20조(개인정보 이동권)■ 전문 제68항, 제73항
------------	--



반대권 (Right to object)



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체의 반대권 행사 요구에 대한 처리 절차 또는 방법을 수립하여 적용하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 온라인 서비스의 경우 정보주체가 온라인으로 반대권 행사를 요구 할 수 있도록 하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

8.1 주요 내용

- 정보주체의 반대권(제21조)은 컨트롤러에 대하여 자신의 개인정보 처리에 반대할 권리를 지칭한다. GDPR은 다음 세 가지 경우에 대하여 정보주체의 반대권을 보장하고 있다.
 - ① 직접 마케팅(프로파일링 포함)
 - ② 컨트롤러의 적법한 이익(제6조제1항(f)) 또는 공적 업무 수행에 근거한 개인정보의 처리(제6조제1항(e))
 - ③ 과학적·역사적 연구 및 통계 목적의 처리

- 정보주체가 반대권을 행사하는 경우 컨트롤러는 문제된 정보를 더 이상 처리하여서는 안 된다. 다만, 반대권 행사 이전에 해당 정보주체의 개인정보에 대한 처리는 여전히 적법한 것으로 유지된다.³⁸

8.2 반대권 요구 시 조치 사항

8.2.1 직접 마케팅을 위한 처리 시

- 정보주체의 반대 요구를 접수한 즉시 컨트롤러는 직접 마케팅(프로파일링 포함)을 위한 개인정보 처리를 중단하여야 한다(제21조제2항). 즉 정보주체가 반대한 후에는 더 이상 직접 마케팅 목적으로 개인정보를 처리할 수 없으며, 그 중단의 범위에는 직접 마케팅과 관련이 있는 프로파일링 행위 역시 포함한다.
- 컨트롤러는 정보주체가 언제든지 직접 마케팅을 위한 처리에 반대 요구를 할 수 있도록 하여야 하며, 이를 무상으로 처리하여야 한다(전문 제70항). 컨트롤러는 개인정보를 수집하는 시점에 정보주체에게 반대권에 대한 내용을 알려 주어야 한다. 이러한 사항은 정보주체에게 명시적으로 강조하여야 하며, 다른 정보와 분리하여 분명하게 제시되어야 한다(전문 제70항).

8.2.2 적법한 이익 또는 공적 업무 수행에 근거한 처리 시

- 개인정보 처리가 다음 두 가지 특수한 목적에 근거한 경우에 정보주체는 자신의 특수한 상황에 대한 이유로 반대권을 행사할 수 있다.
 - ① 제6조제1항(e)에 따른 공익을 위한 업무, 공적 권리를 위하여 필요한 개인정보 처리
 - ② 제6조제1항(f)에 따른 적법한 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 설정(establishment), 행사 또는 방어를 위한 것인 경우

38 FPA, Handbook, pp.231.

8.2.3 과학적·역사적 연구 및 통계 목적의 처리인 경우

- 과학적·역사적 연구 또는 통계 목적으로 개인정보가 처리되는 경우, 정보주체는 자신의 특수한 상황을 이유로 본인과 관련된 개인정보의 처리에 반대할 권리를 갖는다(제21조제6항). 여기서 과학적 연구는 기술적 발전, 기초 연구, 응용 연구, 사적인 자금 지원에 의한 연구를 포함하고, 역사적 연구 역시 통계학적 연구 목적도 포함하는 넓은 개념이며, 통계 목적은 통계 조사나 통계적 결과물을 생산하기 위한 개인정보의 처리를 포함하는 넓은 개념으로 사용 된다.³⁹ 다만 해당 처리가 공익을 위한 업무 수행을 위하여 필요한 경우는 예외로 한다. 한편, 과학적, 역사적 연구 또는 통계목적의 처리가 필요한 경우에는 공익을 위한 것인지의 여부와는 무관하게 삭제권(the right to erasure)은 적용되지 아니한다(제17조제3항(d)).

8.3 온라인 서비스의 경우: 자동화된 방식으로 이의 제기가 가능해야 함

- 컨트롤러는 개인정보의 처리 행위가 반대권을 행사할 수 있는 유형에 속하고 또한 온라인으로 이루어진다면 온라인⁴⁰으로 반대 요청을 처리할 수 있는 방법을 제시하여야 한다. 예컨대 이는 웹 페이지에서 쿠키를 차단하거나 인터넷 브라우저에 대한 트래킹을 차단하는 기능을 포함할 수 있다.⁴¹

GDPR 관련 규정

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

39 GDPR 전문 제159항~제162항.

40 정보사회서비스(Information society services)를 말하며, 전자적 방법으로 서비스 수령자의 요구에 의하여 상업적 목적으로 제공되는 서비스를 지칭한다. Directive 98/34/EC as amended by Directive 98/48/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Art.1(2).

41 FPA, Handbook, p.232.



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.



셀프 체크리스트

Self Check List

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

9.1 프로파일링 및 자동화된 의사결정의 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)
 - 관심사(interests)
- 프로파일링은 ① 자동화된 형태의 정보처리일 것, ② 개인정보에 대하여 수행될 것, ③ 자연인에 대한 개인적 측면들의 평가일 것의 세 가지 요소로 구성된다.
- 자동화된 의사결정이란 인적 개입 없이 기술적 수단(technological means)에 의해서만 이루어지는 완전 자동화 의사결정(solely automated decision-making)을 의미한다.⁴² 자동화된 의사결정은 프로파일링과 무관하게 내려질 수 있고(예컨대, 속도측정 카메라의 증거를 기반으로 속도위반 벌금을 부과하는 경우), 프로파일링에 기반할 수도 있다(예컨대, 개인의 운전습관을 장기간 감시하여 벌금 부과 시 그 액수의 결정에 반복적인 속도위반 내지 운전자의 최근 교통위반 여부를 평가하여 결정하는 경우).

참고

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

이를테면 “서울에 거주하는 여성”과 같은 특정 지역 및 성별 등의 단순 인구 통계학적 정보의 프로파일링을 기반으로 하는 패션 아울렛 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.

42 제29조 작업반, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, 2018. 02. 06., p.7.

9.2 정보 주체의 권리

9.2.1 통지받을 권리

- 컨트롤러는 제22조에서 명시한 정보주체의 권리에 대하여 프로파일링 등이 발생시키는 위험과 간섭을 고려하여 투명성 의무를 특히 엄두에 두어야 한다.
그에 따라 컨트롤러는 제22조제1항에 명시된 자동화된 의사결정을 내리는 경우 아래의 사항을 준수하여야 한다.
 - 정보주체에게 이러한 종류의 활동에 관여하고 있다는 점을 통지하여야 한다.
 - 자동화된 의사결정에 활용된 로직에 대한 의미있는 정보를 제공한다.
 - 정보 처리의 중요성과 예상되는 결과에 대하여 설명해야 한다.

9.2.2 접근 권한의 부여

- 정보주체는 프로파일링을 포함하는 자동화된 의사결정에 대하여 제13조제2항(f)과 제14조제2항(g)에서 요구하는 바와 동일한 정보에 대하여 접근할 수 있는 권한을 갖는다.
 - 프로파일링을 포함하는 자동화된 의사결정의 존재
 - 자동화된 의사결정에 활용된 로직에 대한 의미 있는 정보
 - 정보주체에 대한 이러한 정보 처리의 중요성과 예상되는 결과

9.2.3 프로파일링을 포함한 자동화된 의사결정의 대상이 되지 않을 권리

- 정보주체는 본인에 관하여 ① 법적 효력을 초래하거나 ② 이와 유사한 중대한 효과를 미치는 프로파일링을 포함한 자동화된 처리에 의존된 의사결정의 대상이 되지 않을 권리를 갖는다(제22조제1항).
 - 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 보장 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

※ 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 않는다. 그러나 컨트롤러는 실제적 영향 없이 개인에 대한 자동 생성된 프로파일을 일상적으로 적용하는 경우와 같이 인적 개입의 조작을 통하여 제22조의 적용을 회피할 수 없고, 인적개입은 결정 변경 권한과 능력을 가진 자에 의한 의미 있는 것이어야 한다.⁴³

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

9.3 적용 예외

- 제22조제1항에서 명시하는 프로파일링을 포함한 자동화된 의사 결정에 대한 규정은 다음의 경우 적용되지 않는다(제22조제2항).

- 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 등을 생각해 볼 수 있다. 그러나 이러한 종류의 처리라는 점만으로 그 처리의 충분한 근거는 되지 않고 그 필요성은 좁게 해석되어야 하며, 만약 덜 침해적인 방법을 통하여 동일한 목표를 달성할 수 있다면 프로파일링은 ‘필요’한 것이라고 보기 어렵다.
- ② 그 결정이 유럽연합 또는 회원국 법률에 의하여 허용되는 경우
 - 사기나 탈세 방지 목적, 서비스 보안 및 신뢰성의 보장 등이 포함될 수 있다.
- ③ 그 결정이 정보주체의 명시적 동의에 근거한 경우
 - 다만, 동의 과정에서 프로파일링을 통한 예상 결과 및 관련 정보를 충분히 제공 받아야 하며 선택의 여지없이 서비스 이용을 위하여 동의가 강제되거나, 고용 관계 등 권력의 불균형이 있는 경우의 동의는 적정 동의 절차로 보기 어렵다. 여기서 ‘명시적 동의’는 다른 ‘적극적 행위’(affirmative action) 대신 ‘명시적 진술’을 통하여 구체적으로 입증될 필요가 있다.

43 제29조 작업반, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, 2018. 02. 06., p.8.

참고

아동 대상 자동화된 의사 결정

전문 제71항은 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 제71항의 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.⁴⁴

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.

9.4 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 권리를 보장하고 안전조치를 취하여야 한다.

9.4.1 정보주체 권리 보장 사항

- 컨트롤러는 자동화된 의사결정 내지 프로파일링이 가능한 경우에도 제22조제2항(a) 및 (c)에 의한 경우에는 정보주체에게 최소한 아래의 권리를 보장하여야 한다(전문 제71항).
 - ① 인적 개입을 요구할 권리
 - ② 정보주체가 자신의 견해를 표현할 권리
 - ③ 평가 후의 결정에 대한 설명을 요구할 권리
 - ④ 결정에 대한 이의를 제기할 권리

⁴⁴ 제29조 작업반, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, 2018. 02. 06., p.26.

9.4.2 보호조치

- 컨트롤러가 프로파일링을 위하여 개인정보를 처리할 때에는 다음과 같은 적절한 보호 조치(safeguard)를 적용하여야 한다(전문 제71항).
 - 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

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 정보를 기반으로 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.

9.4.3 개인정보 영향평가(DPIA)⁴⁵

- 프로파일링을 포함한 자동화된 의사 결정에 대해서는 컨트롤러의 책임성을 위해 개인 정보 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 로직(logic) 및 존재에 대한 정보주체 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	<ul style="list-style-type: none">■ 제4조(정의)제4항■ 제22조(프로파일링을 비롯한 자동화된 결정)■ 전문 제71항, 제72항
------------	---

45 제29조 작업반, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation, 2018. 02. 06., p.27.

+ 더 알아보기 / 3

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 자동화된 처리에만 의존한 결정을 거부할 수 있도록 명시하고 있다. 그러나 자동화된 의사 결정과 무관하게 프로파일링만 발생하는 경우에도 GDPR 전반에서 규정하는 개인정보 처리에 관한 주요 원칙 및 정보주체 권리 보장을 위한 관련 조항을 준수해야 한다. 프로파일링만 발생하는 경우나 프로파일링을 포함한 자동화된 의사 결정 모두에 적용되는 조치는 다음과 같다.

#1 개인정보 처리 원칙

원칙	적용 방향
제5조제1항(a) 합법성·공정성·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) 보유기간 제한의 원칙	- 프로파일링을 위한 개인정보를 지나치게 장기간 유지하는 경우 위험을 초래할 가능성이 있으므로 적정 보유기간 산정이 필요

#2 정보주체 권리 보장

원칙	적용 방향
제13조 및 제14조 정보를 제공받을 권리	<ul style="list-style-type: none">- 프로파일링의 프로세스가 어떻게 기능하는지 명확하고 간략하게 설명- 프로파일링을 포함한 자동화된 의사결정 발생 시 ① 프로파일링 사실, ② 프로파일링을 포함한 자동화된 의사 결정 사실 에 대한 정보 제공
제15조 접근권	<ul style="list-style-type: none">- 프로파일링 및 이에 활용된 정보에 대한 정보주체의 접근권 보장
제16조 정정권	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 정보주체의 동의를 받은 프로파일링에 대하여 정보주체가 동의를 철회 할 때, 법적 근거가 있지 않는 한 프로파일링에 사용된 개인정보 및 프 로파일링 결과를 모두 삭제해야 함
제18조 처리 제한권	<ul style="list-style-type: none">- 프로파일링 및 자동화된 의사 결정 과정의 모든 단계에 개인정보 처리 를 차단하거나 제한할 권리를 적용
제21조 반대권	<ul style="list-style-type: none">- 프로파일링을 포함한 자동화된 의사 결정 과정에 대해 정보주체가 대 상이 되지 않을 수 있는 권리를 보장- 프로파일링에 대하여 반대권 제기 시 프로파일링 및 자동화된 의사 결 정을 중단하고 필요할 경우 관련 정보를 삭제



04

기업의
책임성강화



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)



개요



Point

- 개인정보를 처리할 때 준수하여야 하는 7가지 기본 원칙을 이해할 수 있다.
- 이 원칙을 위반할 경우 최고 수준의 과징금이 부과될 수 있다.

- GDPR에서는 기업의 책임성(accountability) 강화를 위한 조항들을 명시하고 있다. 기존의 Directive에서 기업의 책임성 강화는 암묵적인 요구 사항이었으나, GDPR에서는 제5조제2항⁴⁶을 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 요구하고 있다.

| 표 5. 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 최소화하며 궁극적으로는 정보주체의 개인정보보호 권리를 보장하는 데 의의가 있다.

⁴⁶ 컨트롤러는 제5조제1항(개인정보 처리에 대한 원칙)의 준수를 책임지고 이를 입증할 수 있어야 한다.



개인정보 처리 활동의 기록



Point

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



셀프 체크리스트

Self Check List

개인정보 처리 활동의 기록을 준비하기 위하여 다음과 같은 활동을 하고 있는가?	예	아니오
• 우리 조직이 보유한 개인정보를 파악하기 위하여 정규 정보 감사를 실시하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 조직 구성원의 개인정보처리활동을 파악하기 위한 시스템을 갖추고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 보유, 보안, 정보 공유와 같은 영역을 다루기 위하여 조직의 정책, 절차, 계약 및 약정(agreement)을 검토하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 제3자와 공유하는 정보를 수정하는 경우에 해당 제3자에게 알리기 위한 절차를 갖추고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
다음과 같은 개인정보처리 활동에 대해 기록하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 프라이버시 고지(privacy notice)를 위하여 요구되는 정보	<input type="checkbox"/>	<input type="checkbox"/>
• 동의 기록	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러-프로세서 간의 계약 관련 자료	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보의 소재지(location of personal data)	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 영향평가 보고서	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 침해 기록	<input type="checkbox"/>	<input type="checkbox"/>
전자적 수단을 통해 쉽게 개인정보처리활동에 대한 추가, 제거, 수정 등이 가능하도록 구현하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.1 처리 활동 기록이 필요한 경우

- 컨트롤러와 프로세서는 각자 GDPR에 따른 개인정보 처리활동의 기록 의무를 부담한다.

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 기업을 대상으로 개인정보 처리 활동을 의무적으로 문서화하고 보유하도록 규정하고 있다.

2.1.2 예외(종업원 수 250명과 무관)

- 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 있거나 간헐적이지 않은 개인정보 처리
 - ② 민감정보 처리
 - ③ 범죄경력 및 범죄행위에 관련된 개인정보 처리

2.2 처리 활동 기록 대상

- 기업은 내부적으로 다음 내용이 포함된 개인정보 처리 활동을 기록·보유하여야 한다 (제30조).

표 6. 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 개인정보 이전의 경우, 이전 방식에 대한 적절한 보호조치	③ (해당되는 경우) 제3국 또는 국제기구로의 개인정보 이전의 경우, 이전 방식에 대한 적절한 보호조치
⑤ (가능한 경우) 개인정보 유형별 보유기간	
⑥ (가능한 경우) 제32조제1항에 언급된 기술적·관리적 보호조치에 대한 일반적인 설명	④ (가능한 경우) 제32조제1항에 언급된 기술적·관리적 보호조치에 대한 일반적인 설명

- 개인정보 처리 활동의 기록 의무를 이행하는 과정에서 위와 같은 사항 외에도 다음과 같은 사항을 기록하는 것이 유용할 수 있다.

<ul style="list-style-type: none"> • 프라이버시 고지(privacy notice)를 위하여 요구되는 정보 (예) 처리의 합법적 근거, 처리를 위한 적법한 이익, 개인의 권리, 프로파일링을 포함한 자동화된 의사결정의 존재, 개인정보의 수집 출처 등에 대한 프라이버시 고지와 관련한 정보 	<ul style="list-style-type: none"> • 동의 기록 • 컨트롤러-프로세서 간의 계약 관련 자료 • 개인정보의 소재지 • 개인정보 영향평가 보고서 • 개인정보 침해 기록
--	--

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제30조(처리 활동의 기록) ■ 전문 제82항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제29조(안전 조치 의무)



Data protection by design and by default



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보 처리를 위한 서비스를 설계할 때 개인정보 생명 주기 전반에 걸쳐 개인정보가 보호될 수 있도록 구현하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리 시스템과 처리 과정에 개인정보보호 기본 설정(privacy by design & by default)이 반영되어 있는지 점검하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 처리 시스템과 프로세스에 정보의 최소화, 가명처리, 암호화 등의 방법을 포함하는 적절한 기술적·관리적 조치를 실시하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

3.1 ‘Data protection by design and by default’의 의미

- Data protection by design and by default는 캐나다 온타리오주 프라이버시 커미셔너 앤 카부키안(Ann Cavoukian) 박사가 제안한 privacy by design이란 개념으로 처음 소개되었으며, 설계 단계에서부터 기술적으로 프라이버시를 보호하는 구조를 만드는 것을 의미한다.
- GDPR에서는 Data protection by design and by default를 통하여 처리 수단의 결정

시점과 처리 당시 시점에서 개인정보보호의 원칙을 적용하는 데 의의가 있다고 설명한다(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, 개인정보 생명주기 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 보유기간 및 접근 가능성에 대해서도 적용된다.
- Data protection by design and by default의 이행은 정보주체의 개인정보 유출 및 침해와 관련한 위험을 최소화할 수 있고 컨트롤러와 프로세서의 개인정보보호 의무 준수에도 도움이 된다.

⇒ 과징금 부과 사례

1) 그리스 - 통신 서비스 제공 기업 사례⁴⁷

그리스 개인정보 감독기구(HDPA)는 자국의 통신 서비스 제공 기업이 고객 개인정보 처리를 위하여 요구되는 적절한 기술적 조치를 취하지 않음에 따라, 고객의 개인정보가 적절한 시기에 삭제되지 않는 동시에 고객의 opt-out 요구가 반영되지 않은 것을 이유로 과징금 200,000 유로를 부과함(2019. 10.)

2) 루마니아 - UNICREDIT BANK SA 사례⁴⁸

루마니아 개인정보 감독기구(ANSPDCP)는 UNICREDIT 은행 고객의 온라인 ID와 주소가 공개되는 사고가 발생함에 따라, UNICREDIT를 대상으로 데이터 처리를 위한 안전한 기술적·관리적 조치가 충분히 이행되지 않은 것으로 판단하여 과징금 130,000 유로를 부과함(2019. 06.)

⁴⁷ C.M.S law, "GDPR Enforcement Tracker", 2020. 03. 16., <https://www.enforcementtracker.com>

⁴⁸ The National supervisory authority For Personal Data Processing, "FIRST FINE FOR THE APPLICATION OF GDPR", 2020. 03. 17., https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en

3) 폴란드 - 온라인 소매업체 Morele.net 사례⁴⁹

폴란드 개인정보 감독기구(UODO)는 온라인 소매업체 Morele.net이 적절한 기술적 · 관리적 조치를 취하지 않아 발생한 데이터 고객 데이터 유출 사고에 대해 650,000유로의 과징금을 부과함(2019. 10.)

GDPR 관련 규정	<ul style="list-style-type: none">■ 제25조(Data protection by design and by default)■ 전문 제74항~제78항
------------	---

⁴⁹ GDR, <https://globaldatareview.com/article/1197780/poland-hits-shopping-site-with-its-largest-gdpr-fine-to-date>



개인정보 영향평가



Point

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

4.1 개요



셀프 체크리스트

	Self Check List	
	예	아니오
• 개인정보 영향평가의 도입 취지와 필요성을 이해하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 영향평가가 필요한 유형과 절차를 사내 개인정보보호 정책에 반영하였는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.1.1 개인정보 영향평가의 의미

- 개인정보 영향평가(Data Protection Impact Assessment, DPIA)란, ① 개인정보 처리를 분석하고 ② 동 처리의 필요성 및 비례성을 고려하여 ③ 이로 인해 발생하는 자연인의 권리와 자유에 대한 위험을 평가하고 ④ 해당 위험을 다루는 방법을 결정함으로써 그 위험을 관리하기 위해 만들어진 프로세스를 의미한다.

개인정보 영향평가는 컨트롤러의 책임성 이행을 위한 중요한 도구로 개인정보 처리 시 GDPR 요구 사항 준수를 위한 적절한 조치를 취하였음을 입증하기 위해 수행된다.

4.1.2 평가 시 고려 사항

- 개인정보 영향평가 시에는 관련 위험 요소의 출처·성격·특성·심각성 등을 고려해야 한다.
특히 위험을 완화하고 개인정보보호를 보장하며, GDPR 준수를 입증하기 위한 보안 조치, 보호조치 및 개인정보보호 메커니즘이 포함되어야 한다.
영향평가는 조직 내부의 임직원 및 외부인에 의해 실시될 수 있지만 그 책임은 컨트롤러에게 있다.

4.2 개인정보 영향평가 대상



셀프 체크리스트

	Self Check List	
	예	아니오
• 개인정보 처리가 유발되는 사업 추진 시 개인정보 영향평가 대상 여부를 검토하는 절차를 수립하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 영향평가 식별 절차를 사내 정책 혹은 규정에 반영하고 임직원 대상 교육을 실시하였는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.2.1 일반적으로 개인정보 영향평가가 필요한 경우(제35조제1항)

- 새로운 기술을 사용하고 그 처리 유형이 ‘개인의 권리와 자유에 높은 위험’을 초래할 가능성이 있는 경우, 개인정보 처리 이전에 예상되는 개인정보 처리에 대한 영향평가를 수행하여야 한다.

⇒ 개인의 권리 및 자유에 대한 위험의 평가

▷ 주로 개인정보보호 및 프라이버시 권리에 대한 것이나, 표현의 자유, 사상의 자유, 이동의 자유, 차별 금지, 신체의 자유 및 양심과 종교의 자유 등 기본권을 포함할 수 있다.

※ 개인의 권리 및 자유에 대한 높은 위험 발생 가능성의 판단 조건은 [더 알아보기 5] 참고

4.2.2 유사한 영향평가 대상에 대한 일괄 처리(제35조제2항)

- ‘유사한 기술’에 대하여 ‘다수의 컨트롤러’가 영향평가를 받아야 하는 경우 또는 ‘단일 컨트롤러’가 ‘동일하지만 다수의 반복되는 기술 적용’에 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.

4.2.3 개인정보 영향평가를 의무적으로 수행하여야 하는 경우(제35조제3항)

- 특히 다음 중 하나에 해당하는 경우 개인정보 영향평가를 의무적으로 수행해야 한다.
 - ① 자동화된 처리(프로파일링 포함)에 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 범죄정보에 대한 대규모 처리를 하는 경우
 - ③ 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링을 하는 경우(예: CCTV)

4.2.4 개인정보 영향평가 수행이 예외인 경우

- 아래와 같은 경우에는 개인정보 영향평가를 실시하지 않아도 된다.
 - ① 감독기구가 유럽개인정보보호사회(EDPB)에 통보한 개인정보 영향평가가 요구되지 않는 처리 작업 종류 목록에 해당되는 경우(제35조제5항)
 - ② 컨트롤러에게 적용되는 법적 의무 이행을 위하여 필요한 처리나 공익을 위하여 수행되는 직무의 이행 또는 컨트롤러에게 부여된 공적 권한의 행사에 필요한 처리인 경우로 해당 법률에서 특정 처리 작업이나 일련의 관련 작업을 규정하고 있으며 해당 법적 근거 채택 과정에서 개인정보 영향평가가 이미 실시된 경우(제35조제10항)

4.3 개인정보 영향평가 수행 절차



셀프 체크리스트

Self Check List

	예	아니오
•개인정보 영향평가 수행을 위해 개인정보 처리의 성격, 범위, 맥락 및 목적을 기술하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
•개인정보 처리 활동을 이해하고 문서화하여 관련 위험을 식별하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.3.1 평가 내용(제35조제7항)

- 영향평가 수행 시 최소한 다음 내용을 모두 포함하여야 한다.
 - ① 예상되는 개인정보 처리(processing)와 목적에 대한 체계적인 기술
 - ※ (적용되는 경우) 컨트롤러가 추구하는 적법한 이익
 - ② 목적 관련 개인정보 처리 작업의 필요성과 비례성에 대한 평가
 - ③ 정보주체의 권리와 자유에 대한 위험의 평가
 - ④ 개인정보의 보호와 GDPR 준수를 입증하기 위한 보안조치, 보호대책 및 메커니즘 등 위험을 처리할 것으로 예상되는 조치

4.3.2 행동규약의 준수(제35조제8항)

- 영향평가 수행 시 승인된 행동규약의 준수가 고려되어야 한다. 승인된 행동규약은 영향평가가 적합한 수단으로서 선택 또는 시행되었음을 입증하는 데 도움이 된다.

4.3.3 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.

4.3.4 개인정보 영향평가 결과의 공개

- 영향평가 결과는 공개되는 것이 바람직하나 GDPR의 법적 요건은 아니며 컨트롤러의 재량 사항이다. 공개의 목적은 신뢰 증대와 책임감 및 투명성을 증명하기 위한 것이므로 사회 구성원들이 영향을 받는 경우에는 개인정보 영향평가 결과를 공개하는 것이 바람직하다. 개인정보 영향평가 결과를 공개할 때 평가 내용 전체가 포함될 필요는 없다. 컨트롤러의 보안 위험에 관한 구체적 정보를 제시하거나 영업 비밀 또는 상업적으로 민감한 정보를 유출하는 등의 경우가 있을 수 있기 때문이다. 이 경우 영향평가의 주요 결과 또는 단순 수행 여부를 공개하는 것으로 같음할 수 있다.

4.4. 개인정보 영향평가 관련 내·외부 협의 체계



셀프 체크리스트

	Self Check List	
	예	아니오
• 개인정보 영향평가 수행을 위하여 DPO와 사전 협의하는가?	<input type="checkbox"/>	<input type="checkbox"/>
• DPO는 개인정보 영향평가 수행을 모니터링하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 고위험 개인정보 처리 행위에 대한 위험 완화 조치가 미비한 경우 감독기구를 대상으로 사전에 협의하는 체계가 마련되어 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

4.4.1 DPO와 협의가 필요한 경우

- 컨트롤러와 프로세서는 다음과 같은 사항에 대하여 DPO의 조언을 구할 수 있다.
 - ① 개인정보 영향평가 수행 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

4.4.2 감독기구 대상 자문 사전협의가 필요한 경우(제36조)

- 개인정보 영향평가 결과, 개인정보 처리로 인해 발생할 수 있는 위험에 대해 컨트롤러가 충분한 보호조치를 구현하지 못하는 경우 컨트롤러는 그 처리에 대하여 감독기구와 사전에 협의하여야 한다(제36조제1항).

개인정보처리가 회원국 법률의 공익을 목적으로 실시된 경우, 컨트롤러는 영향평가 대신 감독기구와의 사전 협의 혹은 사전 승인을 받고 처리를 진행할 수 있다(제36조제5항).

감독기구는 협의 요청 접수 후 8주 내에 컨트롤러 및 프로세서에게 서면 형식의 권고 사항을 제공할 수 있다. 기간은 최대 6주까지 연장될 수 있으며 한 달 내 지연 사유 및 기간 연장에 대해 알려야 한다(제36조제2항).

- 컨트롤러는 감독기구와의 사전 협의 시 아래 사항을 감독기구에게 제공해야 한다(제36조제3항).
 - ① (가능한 경우) 컨트롤러, 공동 컨트롤러 및 프로세서의 개별 책임, 특히 사업체 집단(a group of undertakings) 혹은 기업 내의 처리에 대한 책임
 - ② 예정된 개인정보 처리의 목적 및 방법
 - ③ 정보주체의 권리와 자유를 보호하기 위해 제공되는 대책 및 안전성 확보 조치
 - ④ DPO 연락처
 - ⑤ 개인정보 영향평가 결과
 - ⑥ 감독기구가 요청한 기타 정보

⇒ 과징금 부과 사례

- 스위스 셀레프테오(Skellefteå)의 한 고등학교는 3주간 22명의 학생에게 안면 인식 기술을 활용하여 학생 출석 확인 시스템을 3주간 테스트하였음
- 이때, 안면 인식에 사용되는 생체정보는 민감정보로 출석 확인의 목적에 활용되는 것은 부적절하며 학생들 대상 카메라 감시로 사용되어 개인의 권리와 자유에 대한 높은 위험을 미쳤음에도 개인정보 처리 활동이나 개인정보 영향평가가 실시되지 않음
- 이에 대해 스위스 감독기구는 제9조 민감정보 처리 위반, 제35조 개인정보 영향평가 의무 위반, 제36조 감독기구 대상 사전 협의 의무 위반으로 2019년 8월 20일 18,630유로의 과징금 부과

⇒ 참고 자료

프랑스 개인정보 감독기구인 CNIL은 개인정보 영향평가 도구를 제작·배포하고 있으며 네이버 프라이버시 센터(privacy.naver.com)에서는 위 도구에 대한 한국어 사용 매뉴얼을 제공하고 있다.

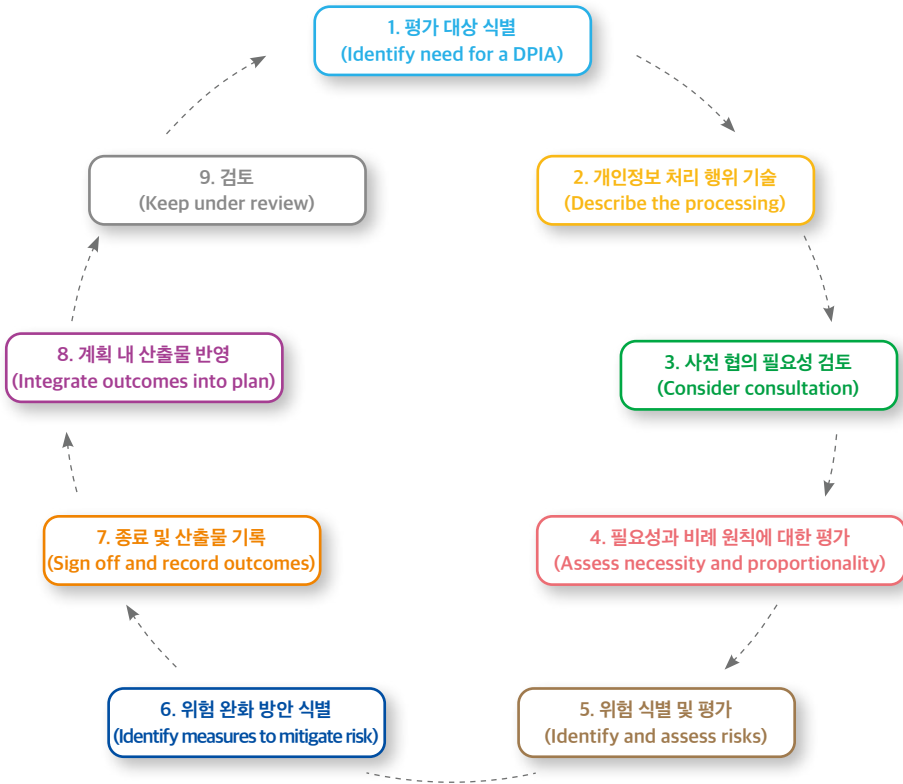
GDPR 관련 규정

- 제35조(개인정보 영향평가)
- 제36조(사전협의)
- 전문 제89항~제94항
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP29

한국 개인정보보호법 관련 규정

- 제33조(개인정보 영향평가)

그림 2. ICO 개인정보 영향평가 절차⁵⁰



50 ICO, "Data protection impact assessments", 2020. 03. 16., <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments>

51 ICO, "Data protection impact assessments", 2020. 03. 16., <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx>

| 표 7. ICO 개인정보 영향평가 양식 예시⁵⁾

[1단계] 개인정보 영향평가 필요성 식별(Identify the need for a DPIA)

- 프로젝트 계획안 등을 참고하여 프로젝트의 목적과 관련 개인정보 처리 유형을 기술
- 영향평가의 필요성을 식별하여 기술

[2단계] 개인정보 처리에 대한 기술(Describe the processing)

- 개인정보 처리의 본질을 기술
 - 개인정보 수집, 이용, 파기 절차, 데이터 출처(source of the data), 제3자 제공 여부 등
 - 개인정보 흐름도 등을 통해 높은 위험 발생 가능성이 높은 단계를 식별
- 개인정보 처리 범위를 기술
 - 데이터의 속성, 민감정보 혹은 범죄 정보 포함 여부, 데이터 수집·이용 규모 및 빈도, 보유기간, 영향을 받는 개인의 수, 처리 지역 등
- 개인정보 처리의 맥락을 기술
 - 정보주체와의 관계, 정보주체의 통제 수준, 정보주체가 기대하는 개인정보 이용 방법, 아동 혹은 취약 집단 포함 여부, 처리 유형별 우려 혹은 보안 취약점, 새로운 유형 여부, 기술 적용 현황, 관련 사회적 이슈, 행동 규약 혹은 인증 획득 여부 등
- 개인정보 처리의 목적을 기술
 - 달성 목표, 의도된 정보주체 대상 영향, 처리의 효용 등

[3단계] 협의 단계(Consultation process)

- 이해 관계자 대상 협의 방안을 기술
 - 관련 임직원의 개별적 의견 수렴 시점 및 방법, 적정성 혹은 부적정 판단 사유, 조직 내 참여가 필요한 임직원의 식별, 프로세서 대상 지원 요청 필요 여부, 정보보안 전문가 등 외부 전문가 대상 자문 여부 등

[4단계] 필요성 및 비례성 평가(Assess necessity and proportionality)

- 특정 사항에 대한 준법성(compliance) 및 비례성(proportionality) 조치 방안을 기술
- 개인정보 처리의 합법성, 개인정보 처리를 통해 달성하고자 하는 목표, 동일한 목표를 위한 다른 방안의 존재 여부, 기능 확대(function creep) 방지 방안, 데이터 품질 보장 및 데이터 최소화 방안, 정보주체 대상 제공 정보 내역, 정보주체 권리 보장 방안, 프로세서 준수 보장 방안, 국외 이전 시 안전성 확보 조치 방안 등

[5단계] 위험 식별 및 평가(Identify and assess risks)

- 위험의 원천과 정보주체 대상 잠재적 영향의 본질을 기술
 - 관련 준법성 및 조직적 위험성을 반드시 포함하여 유해성의 발생 가능성 및 심각성을 기반으로 전체적 위험성을 고-중-저 평가

[6단계] 위험 완화 방안 식별(Identify measures to mitigate risk)

- 고위험 혹은 중위험으로 확인된 위험별로 이를 감소하거나 제거하기 위한 추가적 방안을 식별 및 기술

[7단계] 종료 및 산출물 기록(Sign off and record outcomes)

- 잔여 위험 감소 혹은 제거하기 위한 추가 방안의 승인 내역 및 계획서 내 반영 여부, 잔여 위험 승인 내역 및 고위험에 대한 감독기구 자문 내역, DPO 자문 내역, 외부 전문가의 평가 내역, 개인정보 영향평가 결과에 대한 감독기구 검토 내역 등을 기재



DPO(Data Protection Officer) 지정



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• DPO를 의무적으로 지정해야 하는 경우를 이해하고 있는가? - 정보주체에 대한 '대규모'의 '정기적이고 체계적인 모니터링' - 민감정보 혹은 범죄정보에 대한 '대규모' 처리 - 정부부처 혹은 관련기관의 개인정보 처리	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러 또는 프로세서는 DPO를 지정하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• DPO를 지정한 경우, 법령에서 명시된 DPO의 독립적 지위 및 업무 지원사항을 보장하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러 또는 프로세서는 법령에 따라 DPO의 업무를 명확하게 정의하고 있으며, DPO는 이를 수행하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 컨트롤러 또는 프로세서는 법령에 명시된 업무를 수행할 수 있는 역량을 갖춘 DPO를 지정하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• DPO를 지정한 경우, 컨트롤러 또는 프로세서는 DPO의 연락처 정보를 공개하고, 필요한 경우 감독기구에 통보하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

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.
 - 정부부처 또는 관련기관의 경우(사법적 권한을 행사하는 법원은 예외)
 - 컨트롤러 또는 프로세서의 ‘핵심 활동’이 다음 중 하나에 해당되는 경우
 - ① 정보주체에 대한 ‘대규모’의 ‘정기적이고 체계적인 모니터링’
 - ② 민감정보나 범죄정보에 대한 ‘대규모’의 처리

참고

‘핵심 활동’의 예시

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 개인 정보 처리는 병원의 ‘핵심 활동’ 중 하나인 것으로 본다. 보안 회사의 경우 쇼핑몰 등 공적인 공간을 감시하며, 불가피하게 개인정보의 처리와 연계되어 있다. 이 때 감시는 보안 회사의 ‘핵심 활동’로 본다.

‘대규모 처리’의 의미

GDPR은 대규모(large-scale)의 정의에 대하여 밝히고 있지 않으나, WP29는 처리가 대규모로 수행되는지 여부를 결정하기 위하여 다음의 요소들을 고려할 것을 권고한다.

- ① 관련된 정보 주체들의 수 - 구체적인 수치로서 혹은 관련된 인구의 비율로서
- ② 개인정보의 규모와(또는) 처리되는 다양한 개인정보 항목의 범위
- ③ 개인정보 처리 활동의 기간 또는 연속성
- ④ 처리 활동의 장소적 범위

‘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
- 행태에 따른 맞춤형 광고를 위한 검색엔진의 개인정보 처리
- 전화 또는 인터넷 서비스 제공업체의 개인정보(콘텐츠, 트래픽, 위치) 처리

'정기적'이고 '체계적' 모니터링의 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, 행태에 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 처리와 관련된 업무를 위해 최소 10명 이상의 인력을 고용하는 컨트롤러는 DPO를 의무 지정하도록 명시하고 있다

⇒ 사례

EU 시민을 직접 대상으로 하며, 유럽어를 지원하는 온라인 쇼핑몰의 경우, 혹은 민감정보를 대규모로 처리하는 병원, 쇼핑몰이나 공공장소를 모니터링하는 보안 회사의 경우 DPO를 필수로 지정하여야 한다.

- 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 제37조~제39조가 적용되므로 유의하여야 한다.

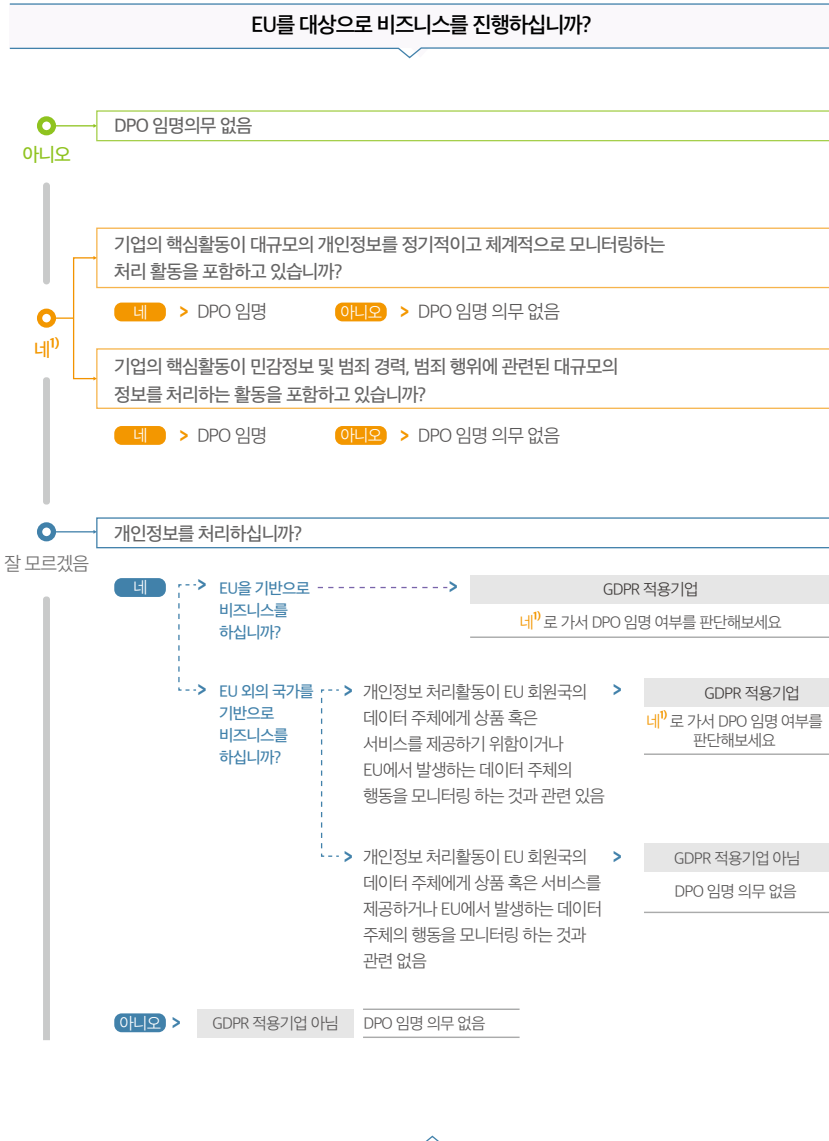
⇒ 과징금 부과 사례

DPO 미지정에 따른 벌금 부과 사례⁵²

오스트리아 개인정보 감독기구(DSB)는 의료 부문에서 운영되는 자국 기업이 DPO 의무 임명 조항을 준수하지 않음에 따라 55,000유로의 과징금을 부과함(2019. 08.)

52 EDPB, "Austrian DPA fines controller in the medical sector", 2020. 03. 15., https://edpb.europa.eu/news/national-news/2019/austrian-dpa-fines-controller-medical-sector_en

| 그림 3. DPO 지정 의사결정 절차



5.1.2 공동 DPO의 지정(제37조제2항)

- GDPR은 ‘각 사업장(establishment)에서 쉽게 접근 가능’하다면, 사업체 집단(a group of undertakings)은 1명의 DPO를 지정할 수 있다고 규정하고 있다. 접근 가능성(accessibility)이란 정보주체, 감독 당국과 관련한 연락 담당, 그리고 조직 내에서 국제적인 접촉점으로서의 DPO의 역할을 말한다.

5.1.3 외부 DPO의 지정(제37조제6항)

- DPO는 컨트롤러 또는 컨트롤러의 직원이거나(내부 DPO), 개인 또는 조직이 서비스 계약에 근거하여(외부 DPO) 직무를 이행할 수 있다.
DPO의 기능이 외부 서비스 조직에 의해 수행될 경우, 각 구성원은 GDPR에서 요구하는 자질을 갖추어야하며 관련 규정에 따라 보호되어야 한다. 법적 명확성과 효율적 조직운영을 위해, WP29는 서비스 계약에 근거하여 외부 DPO 팀 내의 과업을 명확하게 분담 시키고, 대표 연락처 제공 및 고객 대응 ‘담당자’를 지정하도록 권고하고 있다.

5.2 DPO의 자질

- DPO는 제39조에 명시된 업무를 수행할 수 있는 능력을 바탕으로 지정되어야 한다(제37조제5항). 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
- GDPR은 DPO에게 요구되는 전문지식의 수준을 엄격하게 정의하지는 않는다. 하지만 조직이 처리하는 개인정보의 민감성, 복잡성 및 규모에 상응해야 한다. 예를 들어, 개인정보 처리 활동이 특히 복잡하거나 민감한 개인정보가 대량으로 포함되어 있다면, 더 높은 수준의 전문지식이 DPO에게 요구될 수 있다. 또한 조직이 체계적으로 유럽연합 밖으로 개인정보를 이전하는지 혹은 이러한 이전이 가끔씩 일어나는지 여부에 따라 차이가 있을 수 있다.

- GDPR이 DPO의 자질에 대하여 구체적으로 명시하고 있지 않는 반면, WP29의 가이드라인⁵³은 DPO의 전문성(expertise)과 역량(skill)을 다음과 같이 제시하고 있다.

1) 전문 지식 수준(level of expertise)

조직에서 처리하는 데이터의 민감도, 복잡성 및 데이터의 양에 따라 적합한 전문성을 갖추어야 한다. 예를 들어, 데이터 처리 활동이 특히 복잡하거나 많은 양의 민감한 데이터의 처리와 관련된 기업 및 기관의 DPO는 더 높은 수준의 전문 지식이 요구된다.

2) 전문적 자질(professional qualities)

DPO는 자국의 개인정보보호법을 포함하여 유럽 데이터 보호법 및 관행에 대한 전문 지식과 더불어 GDPR에 대한 깊은 이해가 요구된다. 또한 DPO는 수행된 처리 작업뿐만 아니라 정보 시스템, 컨트롤러의 데이터 보안 및 데이터 보호 요구 사항에 대한 충분한 지식이 필요하며, 공공기관의 DPO는 조직의 행정 규칙 및 절차에 대한 올바른 지식이 추가적으로 수반되어야 한다.

3) 작업 수행 능력(ability to fulfill its tasks)

DPO는 데이터 보호 처리 능력 등의 전문적 자질과 지식뿐만 아니라 개인의 청렴함과 높은 수준의 직업윤리를 갖추어야 한다. 이를 통하여 조직 내 문화와 GDPR의 필요요소를 구현하는 기반을 형성하는 데 앞장설 수 있어야 한다.

5.3 DPO의 업무

- DPO는 다음과 같은 업무를 수행하여야 한다(제39조).
 - ① 컨트롤러와 프로세서 및 임직원에게 GDPR과 다른 개인정보 보호법규 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

53 제29조 작업반, Guidelines on Data Protection Officers, 2017. 10. 30.

■ DPO의 역할과 상세 업무를 정리하면 다음과 같다.

DPO 역할	DPO 상세 업무
GDPR 준수 여부에 대한 모니터링	<ul style="list-style-type: none">처리 활동을 식별하기 위한 정보 수집처리 활동에 대한 준수 여부 확인 및 분석컨트롤러 또는 프로세서 대상으로 조언, 자문 제공
개인정보 영향평가에 대한 역할	<ul style="list-style-type: none">개인정보 영향평가 수행 여부 검토개인정보 영향평가 수행을 위한 방법론 검토개인정보 영향평가의 자체수행 혹은 아웃소싱 여부 검토정보주체의 권리와 이익에 대한 위험을 완화하기 위해 적용되는 보호 조치 검토(기술적 · 관리적 보호 조치 포함)개인정보 영향평가의 적절한 수행 여부 및 평가 과정의 GDPR 준수 여부

5.4 DPO의 지위

■ GDPR은 DPO가 개인정보보호와 관련된 모든 문제에 시기적절하게 관여할 수 있도록 보장하여야 한다고 규정한다(제38조). 따라서 기업은 DPO가 개인정보보호와 관련된 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 의무를 이행하기 위하여 필요한 자원을 제공할 것
- DPO가 독립적으로 자신의 과업을 수행하기 위하여 다음의 안전장치가 제38조제3항과 6항에 마련되어 있다.
 - ① DPO의 과업 수행과 관련하여 컨트롤러나 프로세서의 지시를 받지 않음
 - ② DPO 과업의 성과에 대해 컨트롤러가 해고나 처벌할 수 없음
 - ③ DPO 업무 이외의 과업 및 책무와 이해 충돌이 없도록 보장

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.⁵⁴ 즉, GDPR 준수는 컨트롤러나 프로세서의 책임이다.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제37조(DPO의 지정) ■ 제38조(DPO의 지위) ■ 제39조(DPO의 업무) ■ 전문 제97항 ■ Guidelines on Data Protection Officers(DPO) 2016, WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제31조(개인정보 보호책임자의 지정)

⁵⁴ 제29조 작업반, The Guidelines on Data Protection Officer, 2017. 04. 05., p.4.



행동규약과 인증



Point

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



셀프 체크리스트

Self Check List

	예	아니오
• GDPR 준수입증을 위한 수단으로 행동규약 및 인증을 고려하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

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 이 용하도록 권장하고 있다.
- 규약은 컨트롤러 및 프로세서 범주에 대해 특정한 개인정보보호 규칙을 제시하는 자 발적인 책임 도구(tool)이다. 규약은 가장 적합하고 합법적이며 윤리적인 부문의 행 동을 세부적으로 기술한다. 개인정보보호 관점에서, 규약은 유럽 및 각국에 제시된 개 인 정보 보호원칙에 부합하도록 GDPR 준수 정보처리 활동을 설계·실행하는 컨트롤러와 프로세서를 위한 규정서이다.
- 규약은 규칙 설정 기회의 부여 과정을 주된 내용으로 하며, 특정 부문과 처리 활동에 대한 미묘한 차이를 받아들이 수 있도록 하여 실용적이고 투명하며 비용 효율적으로

GDPR을 적절히 적용할 수 있도록 한다. 따라서 규약은 특정 부문에서 실행되는 처리의 구체적인 특징과 중소기업의 구체적인 필요를 고려하여 컨트롤러와 프로세서가 각각 직접 작성할 수 있다. 또한 비용적인 면에서 효과적으로 개인정보보호 준수를 달성할 수 있도록 한다는 점에서 중소기업과 영세기업(micro enterprise businesses)⁵⁵에게 중요하다.

⇒ 사례

보건 연구(health research)를 수행 하는 소규모 기업은 자체적으로 포괄적인 개인정보보호 분석을 수행하기보다는 유관기관 간의 협력을 통하여 건강정보의 수집·처리에 대해 규약을 집단으로 개발할 수 있다. 규약은 특정 직업, 산업 및 기타 분야의 개인정보처리 활동에 대하여 감독 당국이 더 잘 이해하도록 하고 통찰력을 제공한다는 이점이 있다.

⇒ 사례

아동이나 건강정보의 대규모 처리, 자료 수집 또는 체계적인 모니터링과 같이 ‘고위험’ 처리 활동의 경우, 보호에 대한 적정 수준 반응을 위하여 컨트롤러와 프로세서에 더욱더 까다로운 요건이 규약에 포함되도록 하여야 한다.

- 행동규약과 인증제도를 채택하는 경우에는 투명성과 책임성이 향상됨은 물론, 위험을 경감하고 제3자와 계약을 체결할 때에도 행동규약 및 인증제도 확인을 통하여 해당 제3자의 개인정보보호 수준을 파악할 수 있다.

⁵⁵ GDPR 제40조(1)항은 특히 이러한 기업의 필요(needs)를 해결하기 위한 솔루션으로 규약의 필요성을 확인하고 있다.

⇒ 사례

연구 목적용 건강정보(health data) 처리 맥락에서 살펴보면, 승인된 세부 규약으로 민감 건강정보 처리 규칙 준수를 위하여 채택될 수 있는 적정 조치에 대한 우려를 해결할 수 있다. 이러한 규약은 다음과 같은 내용이 포함되어야 한다.

- 정보주체에게 제공되는 정보에 대해 적용할 수 있는 관련 보호장치
- 제3자로부터 취합된 정보에 대해 적용할 수 있는 관련 보호장치
- 정보의 교신 및 확산
- 개인정보 처리의 최소화(data minimisation)를 준수하기 위한 기준
- 구체적인 보안 조치
- 적절한 보유기간
- 정보주체 권리 행사의 결과로서 정보 관리를 위한 메커니즘(GDPR 제32조 및 제89조)

6.2 행동규약의 작성

■ 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 적법한 이익
- ③ 개인정보의 수집
- ④ 개인정보의 가명처리
- ⑤ 일반 대중 및 정보주체에게 제공되는 정보
- ⑥ 정보주체의 권리 행사
- ⑦ 아동에게 제공되는 정보, 그리고 아동에 대한 보호와 부모의 책임을 지닌 자의 아동 관련 동의 획득 방식
- ⑧ 제24조와 제25조에서 규정된 조치 및 절차와 제32조에서 규정된 개인정보 처리의 보안을 보장하는 조치
- ⑨ 감독기구와 정보주체에 대한 개인정보 침해 통지
- ⑩ 개인정보의 제3국이나 국제기구로의 이전
- ⑪ 분쟁 해결 절차

6.3 행동규약 준수에 대한 모니터링

- 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)

- 인증이란, 정해진 인증 기준의 충족 여부에 대한 입증이 이루어졌는지에 대한 평가 및 공정한 제3자의 증명(attestation)⁵⁶을 뜻한다. 기준(criteria) 또는 인증 기준(certification criteria)에 따라 수행⁵⁷ 되는 인증 준수 평가에 의해 이루어진다. 인증 제도는 동일한 특정 요건, 특정 규칙 및 절차가 적용되는 특정 상품, 프로세스 및 서비스와 관련된 인증 시스템을 말한다. 회원국, 감독기구, 유럽 개인정보보호위원회(EDPB) 또는 EU 집행위원회는 투명성과 법령 준수를 향상하기 위한 인증제도 수립을 장려해야 하며, 인증서는 감독기구나 인정된 인증기관이 발행한다.
- 기업은 인증제도를 통하여 기술적·관리적 조치를 실시하고 있음을 보여 줄 수 있으며, 개인정보 역외 이전의 적정성과 관련된 보호조치를 실시하고 있음을 입증할 수 있다. 또한, 특정 제품이나 서비스의 정보보호 수준 평가를 신속히 할 수 있다.
- 인증 메커니즘의 범위는 인증 메커니즘에 따른 개별 인증 평가 대상(target of evaluation, ToE)과 구분되어야 한다.⁵⁸ 인증 메커니즘은 일반적으로 또는 정보 처리 작업의 구체적인 유형 또는 부문과 관련하여 그 범위를 정의할 수 있으며, 어떤 경우이건 준수 여부에 대한 신뢰성 있고 의미 있는 평가는 인증 프로젝트의 개별 대상이 정확히 설명된 경우에만 가능하다. 또한 인증 대상에 어떤 정보 처리 작업이 포함되는지 명확히 설명되어야 하며, 핵심 구성 요소, 즉, 어떤 정보, 프로세스 및 기술 인프라가 평가

⁵⁶ ISO 17000에 따르면 제삼자 증명(attestation, 또는 인증(certification))은 "준수 평가의 모든 대상에 적용되며"(5.5), "단, 인가가 적용되는 준수 평가 기관 자신은 예외로 한다"(5.6).

⁵⁷ GDPR 제42조5항

⁵⁸ 정보 기술 보안 평가에 대한 공통 기준, 1부: 서론 및 일반 모델, 2017.4, 버전 3.1, rev. 5 참조.

되고 어떤 요소들이 제외되는지 설명되어야 한다. 이를 수행함에 있어서 다른 프로세스에 대한 인터페이스가 항상 고려되고 또한 설명되어야 한다. 확실히 알려지지 않은 것은 평가할 수 없고, 따라서 인증을 받을 수 없다.

⇒ 사례

고객들에게 온라인 बैं킹을 위한 웹서비스를 제공하는 경우, 이 서비스의 프레임워크에서는 이체, 주식 매입, 자동 이체, 계정 관리 등이 가능하다. 은행은 일반적인 범위의 개인정보 보호 인증 메커니즘에 따라 아래의 사항을 인증하고자 한다.

a) 보안 로그인

보안 로그인인 최종 사용자가 이해할 수 있으며, 관련 개인정보의 보안을 보장하는 중요한 역할을 수행하므로 정보보호 측면에서 적절한 처리 작업이다. 따라서 이 처리 작업은 보안 로그인에 필수적이며, 인증서에서 로그인 처리 작업만 인증됨을 명확히 나타내는 경우 의미 있는 평가 대상(ToE)이다.

b) 웹 프론트 엔드

웹 프론트 엔드는 정보 보호의 측면에서 적절할 수 있으나, 최종 사용자가 이해할 수 없으며, 따라서 의미 있는 평가 대상(ToE)이 될 수 없다. 또한 최종 사용자는 웹사이트 상에서 어떤 서비스와 처리 작업이 인증의 대상인지 명확히 알지 못한다.

c) 온라인 बैं킹

프론트 엔드는 백 엔드와 함께 온라인 बैं킹 서비스 내에서 제공되는 처리 작업으로 사용자에게 의미가 있을 수 있다. 이러한 맥락에서 웹 프론트 엔드와 백 엔드는 평가 대상(ToE)에 포함되어야 한다. 돈세탁 방지 목적의 처리 작업과 같은 온라인 बैं킹 서비스 제공과 직접 관련이 없는 처리 작업은 평가 대상(ToE)에서 제외될 수 있다.

그러나 은행이 웹사이트를 통해 제공하는 온라인 बैं킹 서비스에는 자체적인 처리 작업이 요구되는 보험 상품의 제공 등이 추가적으로 포함될 수 있다. 이러한 추가 서비스는 온라인 बैं킹 서비스 제공 목적과 직접 관련이 없으므로 평가 대상(ToE)에서 제외될 수 있다. 이 추가 서비스(보험)가 평가 대상(ToE)에서 제외되는 경우, 웹사이트에 통합된 이 서비스에 대한 인터페이스는 평가 대상(ToE)의 일부이며, 이에 따른 서비스 간의 구분을 위해 설명이 이루어져야 한다. 이러한 설명은 두 서비스들 간의 정보 흐름을 식별하고 평가하기 위해 필수적이다.

6.5 인증기관

- 인증기관은 제3자에 대한 준수 평가⁵⁹ 기관⁶⁰(third-party conformity assessment body)으로서, 제42조에 의거한 인증 메커니즘을 운영한다. 의미 있는 인증 메커니즘은 GDPR 준수와 정보주체에 대한 투명성, 그리고 컨트롤러와 프로세서 간의 B2B 관계 투명성을 향상시켜 줄 수 있다.
- 개인정보보호와 관련하여 적절한 수준의 전문 지식을 보유한 인증기관은 필요 시, 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.

GDPR 관련 규정	<ul style="list-style-type: none"> ■ 제40조(행동규약) ■ 제41조(승인된 행동규약의 모니터링) ■ 제42조(인증) ■ 제43조(인증기관)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none"> ■ 제13조(자율 규제에의 촉진 및 지원) ■ 제32조의2(개인정보 보호 인증)

⁵⁹ 제3자 준수 평가 활동은 대상을 제공하는 개인 또는 조직, 그리고 해당 대상에 대한 사용자의 이해로부터 독립적인 조직에 의해 수행된다(cf. ISO 17000, 2.4).

⁶⁰ ISO 17000, 2.5: "준수 평가 서비스를 수행하는 기관", ISO 17011: "준수 평가를 수행하고 인가의 대상이 될 수 있는 기관", ISO 17065, 3.12.

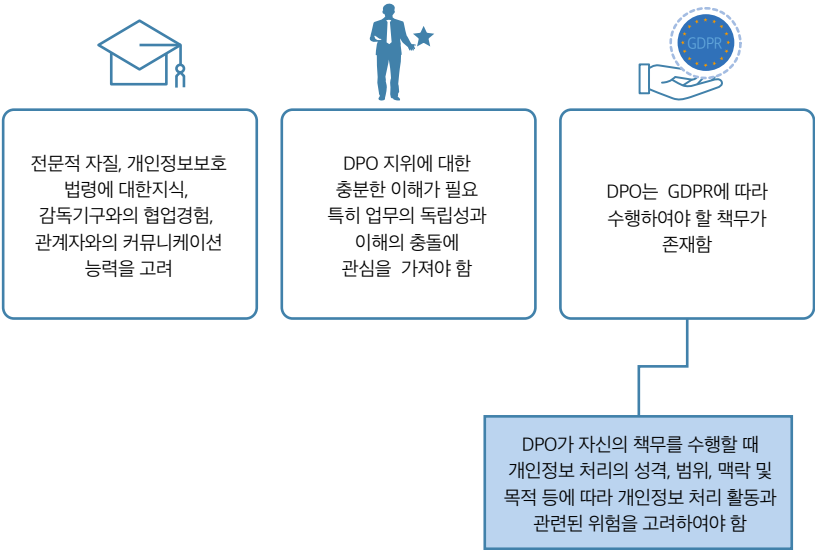
+ 더 알아보기 / 4

DPO 지정 시 고려 사항⁶¹

WP29는 가이드라인을 통해 DPO의 지정이 GDPR 준수에 중요한 역할을 담당하게 될 것이라고 명시하고 있다. GDPR 상에서 특정 컨트롤러와 프로세서는 DPO가 의무 지정 대상이며, DPO의 의무 지정 대상이 아니어도 DPO의 지정은 각 기업의 개인정보 보호 관련 의사결정 시 도움이 될 수 있다.

따라서 WP29에서 제시하는 다음의 고려 사항을 참고하여 DPO를 지정하고 업무 프로세스에 적용할 필요가 있다.

| 그림 4. DPO 지정 시 고려사항



61 제29조 작업반, The Guidelines on Data Protection Officer, 2017. 04. 05.

#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 아니다. 또한 개인정보 역의 이전의 발생 여부에 따라 보다 높은 전문적 자질이 요구될 수도 있다.

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 아니다. 그러나 이러한 사실들이 전문 지식을 보유한 DPO를 확보하였다는 것을 증명하는 데에 도움이 될 수 있다.

DPO는 개인정보 감독기구와 협업한 경험을 갖추어야 한다. 이는 사적으로 감독기구 종사자와 업무 연락을 취할 수 있는 사회적 관계를 요구하는 것이 아니다. 개인정보 감독기구가 추구하는 정책 목표를 이해하고 감독기구가 작동하는 메커니즘을 이해하여 감독기구와의 협업 과정에서 원활한 의사소통을 수행할 수 있는 능력이 필요하다는 것을 의미한다.

DPO는 조직 내부에서만뿐만 아니라, 감독기구 및 정보주체와도 커뮤니케이션을 수행한다. 개인정보 처리로 인해 영향 받는 다양한 관계자와의 커뮤니케이션을 수행하여야 하기 때문에 그 능력이 필수적으로 요구된다. 또한 커뮤니케이션 능력은 EU에서 일반적으로 사용되는 언어 구사 능력이 요구됨을 의미한다. DPO가 EU의 언어를 직접 구사하지 못하는 경우, 조직은 전문적인 통역 자원을 DPO에게 지원하여야 한다.

#2 DPO의 업무 독립성 보장 및 이해 충돌의 방지

DPO는 자신의 책무를 수행하는 것과 관련하여 컨트롤러나 프로세서로부터 어떠한 지시도 받지 않도록 해야 한다. 특히 DPO는 업무 수행과 관련하여 징계를 받거나 해고될 수 없다. 실제 직접적인 징계가 내려지지 않더라도, DPO의 활동과 관련하여 처벌의 가능성을 제시하는 경우에도 징계를 부과한 것으로 이해될 수 있어 주의를 요한다.

DPO는 GDPR이 정한 책무 외에 다른 업무를 수행할 수 있다. 이 때 컨트롤러나 프로세서는 그와 같은 업무가 이해의 충돌(a conflict of interests)을 일으키지 않도록 보장하여야 한다. 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 있다. 컨트롤러나 프로세서는 이와 같은 이해의 충돌이 발생하지 않도록 하여야 한다.

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

#3 DPO의 책무에 대한 이해

DPO는 최소한 다음과 같은 책무를 수행하여야 한다. DPO는 자신의 책무를 수행할 때 개인정보 처리의 성격·범위·맥락·목적 등에 따라 개인정보 처리 활동과 관련된 위험을 고려하여야 한다(제39조제1항).

- ① 컨트롤러나 프로세서, 개인정보를 처리하는 임직원들에게 GDPR 및 EU 회원국의 개인정보보호 규정에 따른 의무 사항을 알리고 조언
 - 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 제시하

도록 권고된다.

- 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 / 5 높은 위험을 초래할 가능성이 있는 개인정보 처리의 판단 기준 9가지

GDPR은 개인정보의 처리가 높은 위험을 초래할 가능성이 있을 경우, 영향평가를 받아 예측되는 위험을 최소화하도록 권장하고 있다.

개인정보 처리 과정에서 높은 위험을 내재하는 개인정보의 판단 기준 9가지는 다음과 같다.⁶² 다만, 하나의 기준만을 충족하는 경우 위험 수준이 높다고 보기 힘들며, 적어도 그 이상을 충족하는 개인정보 처리는 영향평가가 필요한 경우로 볼 수 있다.

| 그림 5. 개인정보 처리 시 높은 위험의 판단 기준



#1 평가 또는 평점

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

62 제29조 작업반, Guidelines on Data Protection Impact Assessment(DPIA) and determining whether processing is 'likely to result in a high risk', (2017. 10. 04., pp.8~12.

#2 자동화된 의사결정에 의한 법적 효과

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

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 때문이다. 또한 공공장소에서 시스템을 통하여 인지하지 못한 대규모 개인정보 처리의 대상이 되는 것을 피하지 못할 수도 있기 때문이다.

#4 민감정보

이것은 제9조에 규정된 민감정보(예를 들면 개인의 정치적 견해에 관한 정보 등) 뿐만 아니라 제10조에 규정된 범죄정보도 포함한다.

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 않다. 다만 WP29는 대규모 처리 여부의 결정에 다음 내용을 고려하도록 권고하고 있다.

- ① 관련 정보주체의 수
- ② 처리하는 정보의 양 또는 서로 다른 정보 유형의 범위
- ③ 정보 처리 활동의 기간 또는 연속성
- ④ 처리 활동의 장소적 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 있다.

#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 있다(아동, 정신질환이 있는 사람, 난민, 노인, 환자, 또는 정보주체와 컨트롤러 간 지위 관계의 불균형이 있는 모든 경우도 포함).

예시

인적 자원 관리와 연계하여 고용주가 처리하는 종업원의 개인정보 등

#8 신기술의 사용 또는 적용

물리적 접근 통제의 개선을 위하여 지문이나 안면 인식 기술을 결합하여 사용하는 것 등이 이러한 사례에 속한다. GDPR은 새로운 기술이 사용됨에 따라 개인정보 영향평가 실시의 필요를 촉발할 수 있다고 명시하고 있다(제35조제1항 및 전문 제89항, 제91항). 왜냐하면 이러한 기술의 이용은 새로운 형태의 정보 수집 및 이용을 내포할 수 있으며, 개인의 권리 및 자유에 대한 높은 위험을 수반할 수 있기 때문이다.

예시

사물인터넷 관련 기술 적용 등 개인의 일상생활 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 포함된다.

예시

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



05

개인정보의
역외 이전



1. 개인정보 역외 이전에 관한 총칙(제5장)
2. EU 역외로 개인정보 이전이 가능한 경우
(제45조~제47조)
3. EU 역외로 개인정보 이전이 가능한 예외적인 특정 상황
(제48조 및 49조)



개인정보 역외 이전에 관한 총칙 (제5장)



Point

- 개인정보 역외 이전의 개념을 이해할 수 있다.
- EU 밖으로 개인정보 이전이 가능한 경우와 요건을 알 수 있다.



셀프 체크리스트

Self Check List


EU 역외로 개인정보를 이전할 수 있는가?	예	아니오
• EEA 밖으로 개인정보 이전을 계획하고 있는가? (예: 다음 문항으로 계속 진행)	<input type="checkbox"/>	<input type="checkbox"/>
• 목적을 달성하기 위해서 개인정보의 이전을 할 필요가 있는가? (아니오: 개인정보 없이 이전할 수 있음) (예: 다음 문항으로 계속 진행)	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보의 수신자가 소재한 국가나 영토, 그 국가의 하나 이상의 특정 영역, 또는 국제기구에 대해 EU가 '적정성 결정(adequacy decision)'을 하였는가? (아니오: 다음 문항으로 계속 진행)	<input type="checkbox"/>	<input type="checkbox"/>
• GDPR에 규정된 '적절한 보호조치(appropriate safeguards)' 중의 하나를 이행하였는가? (예: 개인정보를 이전할 수 있음) (아니오: 다음 문항으로 계속 진행)	<input type="checkbox"/>	<input type="checkbox"/>
• GDPR에 규정된 특정 상황의 예외(제49조)가 적용되는 경우인가? (예: 개인정보를 이전할 수 있음) (아니오: GDPR에 따른 개인정보의 역외 이전은 불가능)	<input type="checkbox"/>	<input type="checkbox"/>
※ 위의 모든 문항을 통해서도 개인정보 역외 이전을 허용하기 위한 법적 근거를 발견하지 못하였다면, GDPR에 따른 역외 이전은 불가능함		

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

※ GDPR 내에서 EU 27개 회원국 및 아이슬란드·노르웨이·리히텐슈타인으로 구성되는 EEA(European Economic Area) 간 데이터 이전은 일반적으로 별도의 보호조치가 불필요하다.

- 여기에는 역외 이전된 개인정보가 다른 제3국이나 국제기구로 재이전 되는 경우 (onward transfer)도 포함된다. 따라서 역외 이전은 여러 국가에서 비즈니스를 운영하는 기업의 경우 중요한 이슈가 될 수 있다. 개인정보를 EU 역외로 이전하기 위해서는 이전하는 정보의 항목, 정보 수출자(data exporter)⁶³, 정보 수입자(data importer)⁶⁴, 이전받는 목적, 정보의 흐름, 적절한 안전 조치 등을 확인하여야 한다.
- GDPR상 역외 이전이 가능한 경우는 다음과 같다.

그림 6. 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 자정 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 폐지개정 또는 정지할 수 있는 권한을 가짐</p>	<p>감독기구의 특정한 승인을 요하지 않는 경우</p> <ul style="list-style-type: none"> 공공기관 또는 기구 간에 법적 구속력이 있는 강제할 수 있는 장치 제47조에 따른 구속력 있는 기업 규칙 집행위원회가 채택한 표준 개인정보보호 조항 감독기구가 채택하고 집행위원회가 승인한 표준 개인정보보호 조항 제40조에 의거하여 승인된 행동규약 제42조에 의거하여 승인된 인증제도 <p>감독기구의 특정한 승인이 필요한 경우</p> <ul style="list-style-type: none"> 컨트롤러나 프로세서와 제3국이나 국제기구의 컨트롤러, 프로세서 또는 개인정보 수령인 간의 계약 조항 행정 합정부 내에 강제력 있고 유효한 정보주체 권리 포함 규정

- ① 적정성 결정(adequacy decision)에 따른 이전(제45조)
- ② 적절한 보호조치에 의한 이전(제46조)
 - 구속력 있는 기업 규칙(binding corporate rules), 표준 개인정보 보호 조항

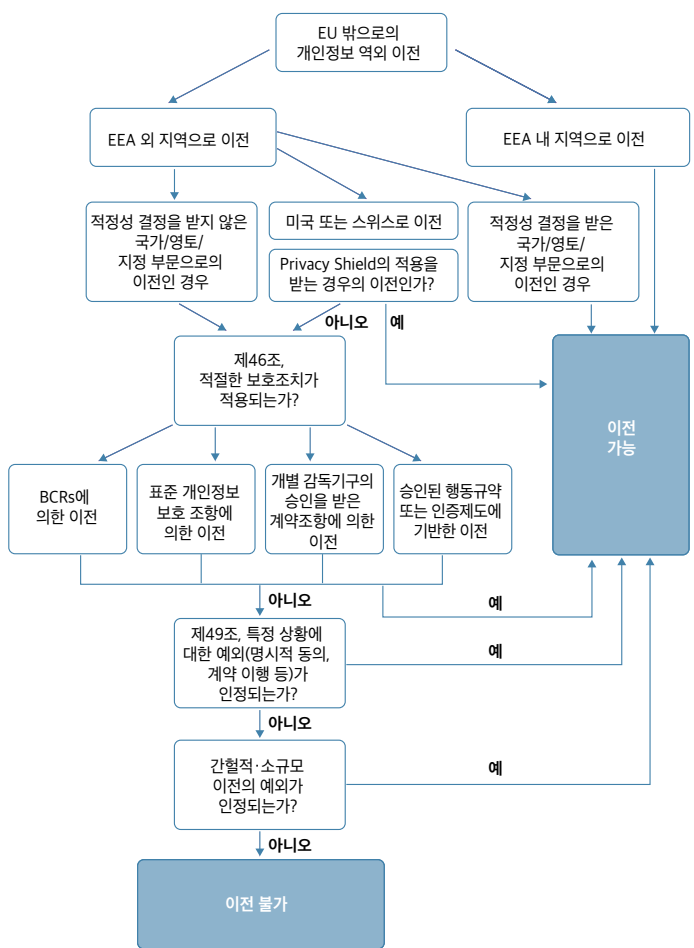
63 EEA 내 사업자 혹은 정보 제공자.

64 EEA 외 사업자 혹은 정보 수령인.

(standard data protection clauses), 인증제도(certification mechanism), 행동규약(code of conduct) 등

- ③ 특정 상황에 대한 예외(derogations for specific situations)(제49조)
 - 간헐적으로 이전이 발생하는 경우로서 적정성 결정이나 적절한 보호조치가 없음으로 인해 발생할 수 있는 위험을 고지 받은 후 정보주체가 명시적으로 동의한 경우 등

| 그림 7. 개인정보 역외 이전 흐름도⁶⁵



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

GDPR 관련 규정

- 제44조(이전의 일반원칙)
- 제45조(적정성 결정에 기초한 이전)
- 제46조(적절한 보호조치에 따른 이전)
- 제47조(구속력 있는 기업규칙)
- 제48조(EU 법에 의하여 허용되지 않는 이전 또는 공개)
- 제49조(특정상황의 예외)
- 제50조(개인정보의 보호를 위한 국제 협력)
- 전문 제26항, 제101~112항, 제114항, 제169항

한국 개인정보보호법 관련 규정

- 제3조(개인정보의 제공) 제3항
- 제14조(국제협력)
- 제39조의12(국외 이전 개인정보의 보호)
- 제39조의13(상호주의)



EU 역외로 개인정보 이전이 가능한 경우 (제45조~제47조)



Point

- 개인정보를 EU 역외로 이전할 수 있는 GDPR의 규정을 이해할 수 있다.
- EU 역외로 개인정보를 이전할 수 있는 조건이나 요건을 이해할 수 있다.



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보를 역외 이전하는 경우, 처리되는 개인정보와 처리 목적을 인지하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보를 역외 이전하는 경우, GDPR에서 허용하는 요건에 의해 이전하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

- EU 역외로 개인정보를 이전하는 경우에 GDPR이 규정하는 적법한 역외 이전의 근거를 충족하여야 한다.
- GDPR의 보호를 받는 EU 내의 개인정보를 GDPR이 적용되지 않는 EU 역외의 수신자에게로 보내거나 접근 가능하게 하는 경우에는 GDPR에 규정된 역외 이전의 법적 근거를 충족하는지를 검토하여 각각의 요건을 충족시켜야 한다.

⇒ 사례

[사례1] 오스트리아 회사는 모회사가 제공하는 미국 소재의 중앙 집중형 인력 관리 서비스(HR)를 이용한다. 오스트리아 회사는 직원들에 대한 정보를 HR과 연결된 모회사로 전송한다. 이 경우 이전에 해당된다.

[사례2] 프랑스 회사가 한국 관광 상품을 판매한다. 예약을 담보하기 위해서 한국의 호텔로 관광 상품을 구매한 고객의 개인정보를 송신한다. 이 경우 역외 이전에 해당된다.

- 단순한 통과(transit)는 역외로의 이전(transfer)에 해당하지 않는다. 즉, 개인정보가 EEA 역내에서 처리되기 위하여 이전되는 중에 단지 전자적으로 EEA 밖의 국가를 통과하는 경우에는 EEA 국가로부터 EEA 밖으로 실제 이전이 일어나지 않는 한 역외 이전에 해당되지 않는다.

⇒ 사례

개인정보가 한국에 있는 서버를 경유하여 프랑스에 있는 컨트롤러로부터 아일랜드에 있는 컨트롤러로 이전되었다. 한국에 있는 동안 개인정보에 접속하거나 조작할 의도가 없다면, 그 이전은 아일랜드로만 이루어지는 것이다.

- 구조화되거나 정렬되지 않은 종이에 있는 개인정보를 수집한 후, 디지털 형태로 만들거나 개인과 관련한 고도로 구조화된 수동 파일링시스템에 넣기 위하여 EEA 밖의 서비스 회사로 보낸다면 역외 이전에 해당한다.

⇒ 사례

독일 보험 중개인이 개인 고객에 대한 다수의 종이 노트를 한국에 있는 회사로 보낸다. 이 종이 노트는 수기로 작성되었고 컴퓨터에 저장되거나 특정 순서로 보유되지도 않았다. 한국에 있는 회사는 종이 노트를 컴퓨터 고객 관리 시스템에 입력한다. 이 경우는 역외 이전에 해당한다.

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

- EU 집행위원회(European Commission)가 제3국(제3국의 영토, 하나 이상의 지정 부문 포함) 또는 국제기구에 대하여 적정한 보호 수준을 보장한다고 결정한 경우, 적정성 결정을 근거로 제3국 또는 국제기구로의 개인정보 이전이 가능하다.

- EU 집행위원회는 보호 수준을 평가할 때 초기결정을 마련한 후, EDPB와 유럽의회 LIBE 상임위(European Parliament Committee on Civil Liberties, Justice and Home Affairs)등의 검토 및 의견 수렴 등을 진행하며, ‘적정성 결정’이 최종 승인된 이후 최소 4년마다 정기적인 검토를 실시하여야 한다. 집행위원회는 적정성 결정을 폐지·개정·정지 할 수 있는 권한을 갖는다.
- 2022년 11월 현재까지 우리나라를 비롯해 안도라, 아르헨티나, 캐나다(상업적 조직), 파로 아일랜드, 건지(Guernsey), 이스라엘, 맨 섬(Isle of Man), 일본, 저지(Jersey), 뉴질랜드, 스위스, 영국, 우루과이, 미국(Privacy Shield 체계에 한정)에 대한 적정성 결정이 있었다.
- 적정성 결정이 내려지면, 그 효과로서 EU로부터 제3국으로 추가적 안전조치 없이도 개인정보를 이전할 수 있다. 즉, EU 역외의 적정성 결정을 받은 국가로의 개인정보 이전은 EU 역내에서의 개인정보의 이전과 유사하게 취급된다.

| 표 8. EU 적정성 결정 절차

1단계	2단계	3단계	4단계	5단계
EU 집행위의 초기결정 (초안 발표)	EDPB 의견 수렴	커미톨로지* 절차 : EU 회원국 대표자 위원회 심의·의결	유럽의회 LIBE 위원회 업데이트	EU 집행위원회의에서 최종 결정

* 커미톨로지(Comitology) : 공동 결정을 도출해 내기 위해 EU 회원국 대표자와 집행위원회로 구성된 정책 결정 및 집행기구

2.2 우리나라의 EU 적정성 결정(adequacy decision) 획득

- 우리나라와 EU는 2021년 12월 17일 「개인정보보호 적정성 결정(Adequacy Decision)」이 채택되고 즉시 발효됨을 상호 확인하고 언론을 통해 공개 발표하였다.
- 이에 따라 우리나라가 개인정보 국외이전에 있어 EU회원국에 준하는 지위를 부여받게 되었고, 우리 기업들의 경우 표준계약조항(Standard Contractual Clauses, SCC)

등 기존의 까다로운 절차가 면제된다.

- 그간 EU에 진출한 우리나라 주요기업들은 주로 표준계약 등을 통해 EU 개인정보를 국내로 이전하여 왔으며, 이를 위해 많은 시간과 비용을 투자하여 왔음에도 불구하고 GDPR 관련 규정 위반에 따른 과징금(최대 전 세계 매출 4%) 부과 등에 대한 큰 부담을 안고 있었다. 또한 중소기업의 경우에는 표준계약절차 자체가 어려워 EU 진출을 미리 포기하는 사례도 많았다.

⇒ 사례

[사례1] 한국계 기업이 EU에 지사를 둔 경우(반대의 경우도 동일)

- (적정성 결정 채택 以前) 프랑스 파리에 소재하는 A사(지사)는 EU 고객을 대상으로 맞춤형 쇼핑 대행업(특히 한국 상품)을 하고 있는데, 고객들이 선호할 것으로 예상되는 상품을 선정하기 위해 고객의 개인정보를 자체 분석하는데 어려움이 있어 한국 본사에 분석을 의뢰해 왔다. EU 고객정보를 한국으로 이전하기 위해서는 표준계약조항을 활용할 수밖에 없어, 시간·비용 부담 및 법 위반 우려*로 인해 소극적으로 영업 활동을 하였다.

* 프랑스 개인정보감독기관(CNIL)으로부터 표준계약조항 관련 GDPR 규정 위반 여부 조사 및 과징금(최대 전 세계 매출액 4%) 처분을 받을 우려

- (적정성 결정 채택 以後) 한국에 대한 적정성 결정으로 인해 A사는 한국 본사로 EU 고객정보를 보내는 과정이 간소화되었으며, 표준계약조항을 이용하지 않아도 됨에 따라 비용·시간 및 법적리스크 감소로 적극적인 영업 활동이 가능하게 되었다.

[사례2] EU 기업과 한국 기업 간에 개인정보가 이전되는 경우

- (적정성 결정 채택 以前) 독일에 소재하는 B사(독일 기업)는 고객 개인정보를 분석하여 새로운 마케팅 전략 수립이 필요한 상황이었다. 그러나 이에 특화된 전문성 있는 데이터 연구 기업을 EU 내에서는 찾기 어려워 한국으로 데이터를 이전하여 처리하고자 하였으나 표준계약 등으로 인한 부담이 있어 제한적인 연구만 가능했다.
- (적정성 결정 채택 以後) 한국에 대한 적정성 결정으로 인해 한국으로의 개인정보 이전이 자유로워짐에 따라 B사는 한국의 전문성이 있는 데이터 연구 기업과의 제휴가 보다 확대되었다.

2.3 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 개인정

보를 이전할 수 있다.

2.3.1 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 집행할 수 있는 장치
 - 정부부처 또는 관련기관 간 법적 효력을 전제로 하는 협약 등을 예시로 들 수 있다.
 - ② 제47조에 따른 구속력 있는 기업 규칙(BCR, Binding Corporate Rules)
 - 다국적 기업이 제47조를 준수한 BCR을 채택하고 EU 내 감독기구의 승인을 받는 경우, 제3국에 위치한 그룹사로 이전하는 것이 가능하다.
 - ③ 표준 개인정보보호 조항(Standard Data Protection Clauses) 또는 표준계약조항⁶⁶
 - SCC에 의해서도 개인정보 역외 이전이 가능하다.
 - SCC는 EEA 역내의 컨트롤러/프로세서(개인정보 수출자, data exporter)와 역외 제3국의 컨트롤러/프로세서(개인정보 수입자, data importer)간에 개인정보 역외 이전 계약 체결을 위하여 사용되는 통일된 양식의 정보 이전 조항으로 수출자와 수입자가 컨트롤러나 프로세서냐에 따라 4가지 모듈로 구분된다.⁶⁷
 - SCC는 1) 기존의 EU집행위원회가 채택하거나, 2) 감독기구가 채택하고 EU집행위원회가 승인한 조항으로 수정·교체·폐지되지 않는 한 그대로 인정된다.(더 알아보기 6> 참조)

66 GDPR은 표준 개인정보보호 조항이 Standard Data Protection Clauses로 규정되어 있지만, GDPR 이전 개인정보보호 지침(Directive 95/46/EC, 이하 지침)부터 SCC(Standard Contractual Clauses)라는 용어가 널리 활용되어 왔기 때문에 이 가이드북에서는 SCC로 약칭

67 SCC는 기존에 EEA 역내의 컨트롤러와 역외의 컨트롤러 또는 프로세서로 이전되는 경우에 대해 3가지 유형의 조항(문서)이 있었으나, 2021년 6월 이를 통합 개정해 하나의 조항(문서)에서 4가지 유형을 모두 다루고 있음. 여기에서 4가지 유형이란 수출자와 수입자의 자격에 따라 컨트롤러-컨트롤러(모듈1), 컨트롤러-프로세서(모듈2), 프로세서-프로세서(모듈3), 프로세서-컨트롤러(모듈4)의 구분되는 경우임

표 9. 표준계약조항(SCC)에서 구분하는 4가지 모듈과 상황

모듈	수출자	수입자	개인정보 역외 이전 상황
모듈1	컨트롤러	컨트롤러	개인정보가 EU 역내의 컨트롤러로부터 EU 역외의 컨트롤러로 이전되는 경우
모듈2	컨트롤러	프로세서	개인정보가 EU 역내의 컨트롤러로부터 EU 역외의 프로세서에게로 이전되는 경우
모듈3	프로세서	프로세서	개인정보가 EU 역내의 프로세서로부터 EU 역외의 프로세서에게로 이전되는 경우
모듈4	프로세서	컨트롤러	개인정보가 EU 역내의 프로세서로부터 EU 역외의 컨트롤러로 이전되는 경우

④ 제40조에 따라 승인된 행동규약

- 컨트롤러와 프로세서를 대변하는 협회와 기관 등은 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

GDPR 관련 규정

- 제45조(적정성 결정에 기초한 이전)
- 제46조(적절한 보호조치에 따른 이전)
- 제47조(구속력 있는 기업규칙)
- 전문 제26항, 제101항~제112항, 제114항, 제169항



EU 역외로 개인정보 이전이 가능한 예외적인 특정 상황 (제48조 및 제49조)



Point

- 개인정보를 EU 밖으로 예외적으로 이전할 수 있는 GDPR의 규정을 이해할 수 있다.
- EU 밖으로 개인정보를 예외적으로 이전할 수 있는 조건이나 요건을 이해할 수 있다.

- GDPR 제45조부터 제47조까지에 따른 개인정보의 역외이전 사유가 없다고 하더라도, 예외적인 특정 요건이 충족되는 경우에는 개인정보의 역외이전이 허용된다.

EU 법에 의하여 허가되지 않은 이전 또는 공개라고 하더라도, 컨트롤러나 프로세서가 개인정보를 이전하거나 공개할 것을 요구하는 제3국의 사법부의 판결 또는 행정당국의 결정은 국제 협정(international agreement)에 기초한 경우에는 유효하며 집행할 수 있다. 예외적으로 역외 이전이 허용되는 국제 협정의 예로서 개인정보의 역외 이전을 요청하는 제3국 및 EU·EU회원국 사이의 유효한 상호 사법 공조 조약이 있다. 구체적으로는 승객 이름 기록(Passenger Name Records, PNR)에 관한 호주, 미국, 캐나다와의 국제협정이나 테러 자금 추적 프로그램(Terrorist Financing Tracking Programme, TFTP)이 있다.

- 적정성 결정, 적절한 보호조치가 없는 경우 제3국이나 국제기구로의 개인정보 이전 시 다음의 특정 상황에 대하여 예외를 두고 있다(제49조제1항).⁶⁷

- ④ 정보주체가 적정성 결정 및 적절한 보호조치가 없음으로 인해 정보주체에게 발생할 수 있는 정보 이전에 대한 위험을 고지 받은 후, 정보주체가 이전에 명시적으로 동의한 경우

⁶⁷ 제29조 작업반, Guidelines on Article 49, Derogations for specific situation., 2018. 02. 06.

예시

개인정보 역외 이전 시의 명시적 동의⁶⁸

- 개인정보의 역외 이전에 대한 명시적 동의를 받기 위해서는 정보주체에게 해당 국가 또는 지역의 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 수입자와 그 유형, 이전되는 정보의 유형, 정보가 이전될 국가 등
- 해당 내용에 대한 명확한 고지와 정보주체의 인지가 전제되어야 정보주체의 명시적 동의에 의한 역외 이전이 가능하다

- ① 정보주체와 컨트롤러 간 계약 이행을 위하여 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위하여 정보 이전을 하여야 하는 경우
 - ② 정보주체의 이익을 위하여 컨트롤러와 그 밖의 개인이나 법인 간 체결된 계약의 이행을 위하여 정보 이전을 하여야 하는 경우
 - ③ 중요한 공익상 이유로 정보 이전이 반드시 필요한 경우
 - ④ 법적 청구권의 입증(establishment), 행사나 방어를 위하여 정보 이전이 필요한 경우
 - ⑤ 정보주체가 물리적 또는 법률적으로 동의할 수 없는 경우, 정보주체 또는 다른 사람의 중대한 이익을 보호하기 위하여 정보 이전이 필요한 경우
 - ⑥ EU 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반적으로 대중 또는 적법한 이익을 입증할 수 있는 제3자에 의한 협의를 위하여 공개되는 등록부로부터 이전되는 경우로서 EU 또는 회원국 법률에 규정된 협의 조건이 충족되는 범위 내에서 이전되는 경우
- 위의 조건(제49조제1항(a)~(g)), 적정성 결정(제45조) 또는 적절한 보호조치(제46조)에 따른 이전에 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 적법한 이익의 목적에 필요한 경우

68 제29조 작업반, Guidelines on Article 49, Derogations for specific situation, 2018. 02. 06., pp.6~8.

③ 컨트롤러가 개인정보 이전과 관련한 일체의 상황을 평가한 후 그 결과를 토대로 적절한 보호조치를 제시하는 경우

- 다만 이러한 경우에도 컨트롤러는 의무적으로 해당 감독기관에 이전에 대하여 통지하여야 한다.
- GDPR 제49조(특정 상황에 대한 예외)는 개인정보 역외이전에 대한 특례 규정이므로 엄격하게 해석되어야 하며, 제5조 및 제6조에 따른 개인정보 처리의 일반 원칙과 합법 처리 근거를 준수하여야 한다.

특히, 정보이전이 간헐적이고 반복적이지 않으며, 한정된 숫자의 정보주체에만 적용되어야 한다. 고용계약과 같은 안정적인 관계에서의 인사 및 급여 등의 정보 전송은 간헐적인 이전에 해당되지 않는다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 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 제103항~제114항
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제17조(개인정보의 제공)제3항

+ 더 알아보기 / 6

표준 개인정보보호 조항(SCC)

#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 의미한다. 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 인정된다.

EU 집행위원회는 총 세 가지의 표준 개인정보보호 조항 양식을 채택하고 있다.⁶⁹ 두 개는 'EU 역내의 컨트롤러-EU 역외의 컨트롤러 간' 계약 조항이고, 다른 하나는 'EU 역내의 컨트롤러-EU 역외의 프로세서 간' 계약 조항이다.

#2 표준 개인정보보호 조항의 내용

표준 개인정보보호 조항의 세부 내용은 EU 개인정보보호 원칙을 명시하고 있으며, 계약서의 유형과 관계없이 계약 당사자는 공통적으로 다음 내용을 작성하여야 한다.

- ① 정보 수출자(data exporter)와 정보 수입자(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 권리를 보장하고 컨트롤러의 의무를 준수해야 한다.

⁶⁹ 현재 사용되고 있는 표준 개인정보보호 조항은 EU 집행위원회 홈페이지(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, BCR에 비해 비교적 쉽고 간단하다.

- 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 완료되었는지 에 대한 검토를 함께 진행하여야 함

- ② 정보 수입자의 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 된다.

#4 표준 개인정보보호 조항의 장점 및 단점

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

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

정보 수출자(data exporter)와 정보 수입자(data importer)가 별도의 법인격으로 구분되지 않는 경우에는 계약을 체결하기 곤란하다는 점도 단점으로 꼽힌다.

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

+ 더 알아보기 / 7

구속력 있는 기업 규칙(Binding Corporate Rules, BCR)

#1 BCR

BCR은 다국적 기업 내부에서 발생하는 개인정보의 역외 이전을 위하여 기업에서 정한 법적 구속력을 갖춘 내부 관리 규정을 의미한다. 기업에서 채택한 기업 규칙이 법적 구속력을 갖추기 위해서는 관할 감독기구의 승인이 필요하다.

기업이 EU의 개인정보보호 원칙을 준수한 기업 규칙을 작성⁷⁰하여 감독기구에 승인을 요청하면, 감독기구는 자체 검토 및 유관 감독기구의 회람을 통하여 해당 규칙의 적합성을 판단한다. 검토 결과 해당 기업규칙이 개인정보보호에 필요한 조치를 갖추었다고 인정되면, 다른 회원국 감독기구들도 이를 따라 인증하게 되는 시스템이다.

BCR은 해당 기업 규칙이 적용되는 기업 집단의 모든 구성원에게 공동으로 적용된다. 따라서 다국적 기업이 BCR을 승인받으면 영업 활동이 진행되고 있는 국가의 보호 수준과 무관하게 기업 내 개인정보 역외 이전이 가능하게 된다.

#2 BCR의 승인 요건

BCR이 일관성 메커니즘에 따라 감독기구로부터 법적 구속력을 인정받기 위해서는 크게 다음 세 가지 기준을 충족시켜야 한다.

- ① BCR이 법적 구속력을 가지고 기업집단 또는 공동 경제 활동에 종사하는 사업자의 집단과 관련된 모든 구성원(종업원을 포함)에게 적용되고, 준수되어야 한다.
- ② BCR이 개인정보의 처리와 관련하여 정보주체에게 집행할 권리를 명시적으로 부여하여야 한다.
- ③ BCR이 제47조제2항에서 정하는 요건을 충족하여야 한다.

BCR은 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 바람직하다.

70 BCR 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).

BCR에 반드시 기재되어야 하는 사항은 다음과 같다.

- ① 기업집단 또는 공동 경제 활동에 종사하는 사업자의 집단 및 각 구성원의 체제와 연락처 정보
- ② 개인정보의 유형, 처리의 종류와 목적, 영향을 받는 정보주체의 유형 및(개인 정보 이전 대상) EU 역외의 해당 제3국 또는 다수의 제3국의 특정 정보를 포함한 개인정보 이전 또는 일련의 개인정보 이전
- ③ 내·외부적인 법적 구속력
- ④ 일반적인 개인정보 보호 원칙의 적용. 특히 목적 제한, 개인정보 최소화, 보존 기간 제한, 개인정보 품질, Data protection by design and by default, 처리에 관한 법적 근거, 민감정보 처리, 개인정보 보안을 보장하기 위한 조치 및 BCR에 의해 구속되지 않는 단체로의 재이전시 요구사항
- ⑤ 처리에 관한 정보주체의 권리 및 그러한 권리의 이행 수단. 제22조에 따른 프로파일링을 포함한 자동 처리만에 의한 의사결정에 반대할 권리, 관찰 감독 당국에 불복할 권리, 제79조에 따라 회원국의 관할 법원에 소송할 권리, 시정 요구 권리 및 적절한 경우에는 BCR의 침해에 대한 보상을 받을 권리를 포함
- ⑥ EEA 내에 거점이 없는(개인정보 이전에) 관련된 모든 구성원이 BCR의 모든 위반에 대한 책임을 회원국의 영역에 거점을 갖는 컨트롤러 또는 프로세서가 맡을 것. 컨트롤러 또는 프로세서는 해당 구성원이 손해를 발생시킨 사건에 책임이 없다고 증명하는 경우에만 전체 또는 일부 해당 책임이 면제되는 것으로 할 것
- ⑦ 개인정보 주체에 대한 BCR 통지 방법
- ⑧ 제37조에 따라 선임된 모든 DPO 또는 기업집단 또는 공동 경제 활동에 종사하는 사업자의 집단에서 BCR의 준수 및 교육, 이의 제기 처리를 감시하는 역할을 하는 기타 사람 또는 사업체의 업무
- ⑨ 민원 절차
- ⑩ BCR의 준수를 확실히 검증하는 기업집단 또는 공동 경제 활동에 종사하는 사업자 집단의 구조
- ⑪ BCR 규정 변경을 보고, 기록하고 해당 변경 사항을 감독 당국에 보고하는 방법
- ⑫ 기업집단 또는 공동 경제 활동에 종사하는 사업자 집단의 모든 구성원이 확실하게 BCR을 준수하기 위해 필요한 감독 당국과의 협력 구조

- ⑬ BCR에서 제공하는 보장에 실질적으로 악영향을 일으키는(非 EU) 제3국의 기업집단 또는 공동 경제 활동에 종사하는 사업자 집단의 구성원에 적용되는 모든 법적 요구 사항을 관할 감독 당국에 보고하는 방법
- ⑭ 개인정보에 항상 또는 정기적으로 접근하는 인력에 대한 적절한 교육

#3 BCR의 승인 절차

기업의 BCR이 법적 구속력을 갖추기 위해서는 다음 절차에 따라 감독기구의 승인을 받아야 한다.

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

#4 BCR의 장점 및 단점

BCR은 하나의 기업 집단 내에서 발생하는 개인정보 이전에 대한 포괄적인 적합성을 인정받을 수 있다는 장점이 있다. 즉 하나의 기업 집단 전체에 적용되는 보호조치이기 때문에 여러 국가에서 영업 활동을 펼치고 있는 다국적 기업의 정보 이전 활동에 특화되어 있다.

그러나 BCR의 승인을 받는 데 상대적으로 긴 시간과 예산·인력 등이 소요된다는 단점이 있다. 또한 그룹 외부의 기업에 대한 적용이 불가하여 별도의 보호조치를 추가로 준비해야 하는 점도 BCR의 단점 중의 하나이다.

#5 참조할 만한 BCR 사례

승인받은 기관	감독기구	URL
eBay	Luxembourg DPA	https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-korean.pdf (한국어 BCR)
First Data	UK ICO	https://www.firstdata.com/downloads/legal/fd-bcr-summary.pdf
HP	CNIL	https://www8.hp.com/uk/en/pdf/privacy/HPBinding-Corporate-Rules.pdf
Intel	UK ICO	https://blogs.intel.com/policy/files/2012/01/IntelCorporatePrivacyRules.pdf
JPMorgan Chase	UK ICO	https://www.jpmorgan.com/jmpdf/1320746604650.pdf
Philips	UK ICO	https://www.philips.com/c-dam/corporate/about-philips/investor-relations/General-Business-Philips-PrivacyRulesCSBData.pdf

#6 BCR 현황 : 2018년 5월 기준 132개 기업이 BCR 승인을 받음⁷¹

71 European Commission, List of companies for which the EU BCR cooperation procedure is closed, 2020. 03. 17., https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en



06

개인정보 침해발생시
조치사항



1. 개인정보 침해
(Personal Data Breach)
2. 개인정보 침해 통지
(Personal Data Breach Notification)



개인정보 침해



Point

- 개인정보 침해의 개념과 위험성을 이해할 수 있다.

1.1 개인정보 침해의 개념



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보 침해 사고의 개념과 유형을 이해하고 사고 여부를 판단하는 기준을 수립하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 침해 사고가 개인정보의 손실 혹은 유출만을 의미하지 않는다는 것을 이해하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.1.1 개인정보 침해(Data breach)란 무엇인가?

- 개인정보 침해는 개인정보의 파괴(destruction), 손실(loss), 변경(alteration), 인가받지 않은 공개 또는 접근(unauthorized disclosure or access)⁷²을 일으키는 보안 위반(a breach of security)을 의미한다.

72 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

1.1.2 개인정보 침해의 유형

- 개인정보의 침해는 보안의 3요소(기밀성·가용성·무결성)에 따라 다음과 같이 구분할 수 있다.

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 우발적으로 또는 비인가자에 의해 삭제되거나 암호화된 정보에 대한 복호화 키가 분실된 경우 - 정전 또는 DDoS 공격 등으로 조직의 일반적인 서비스에 대한 심각한 중단이 발생하여 항구적 또는 임시적으로 개인정보가 가용하지 않게 되는 경우 등
무결성 침해 (Integrity breach)	개인정보에 대한 허가받지 않은 또는 우발적인 변경이 있는 경우	- 공격자에 의해 개인정보가 변경 또는 오염되었거나, 더이상 완전한 상태가 아닌 경우 등

1.1.3 개인정보 침해 사고로 발생 가능한 위험의 이해

- 개인정보 침해 사고 중 정보주체 권리와 자유에 미치는 위험이 있는 경우에만 감독기구 및 정보주체 대상 통지가 필요하므로 개인정보 침해 사고로 발생 가능한 위험의 개념을 이해하는 것이 중요하다.
- 개인정보 침해 사고로 발생 가능한 위험이란, 개인정보 침해가 시의적절(timely manner)하게 해결되지 않을 경우 초래되는 신체적·물질적·정신적 손해(damage)로써 정보주체의 개인정보에 대한 통제권 상실, 권리의 제한, 차별, 신분 도용 및 신용 사기, 금전적 손실, 가명 정보의 비인가 재식별(unauthorized reversal of pseudonymisation), 명예 훼손, 직무상 비밀로 보호되는 개인정보의 기밀성 상실과 그 밖의 경제적·사회적 불이익 등이 해당된다(전문 제85항).

1.2 개인정보 침해 사고의 인지



셀프 체크리스트

Self Check List

	예	아니오
• 개인정보 침해 사고 발생 대응을 위한 계획을 수립하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 유관 임직원 혹은 부서를 대상으로 사고 관리에 대한 책임을 할당하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 임직원은 보안 사고 발생 시 의사 결정을 위한 보고 대상 임직원 및 부서에 대해 인지하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 이상 경보 발생시 개인정보 침해 사고 여부로 판단하기 위한 상세 조사 절차가 마련되어 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

1.2.1 개인정보 침해의 인지

- 개인정보 침해 사고를 ‘인지(aware)’한 이후 부당한 지연없이(without undue delay) 72시간 내 통지가 필요하므로 인지 시점의 판단이 중요하다.
- 최초 경보(initial alert) 이후 실제 개인정보 침해 여부를 판단하기 위한 자체 조사 기간은 인지 시점이 아닐 수도 있다. 예를 들어, 고객 및 언론 등 외부로부터 개인정보 침해 가능성을 통지받았거나 네트워크 로그 모니터링을 통해 이상 징후가 탐지된 경우 이 같은 경보가 실제 보안사고 발생을 의미하는지 보안사고 발생으로 인해 개인이 영향을 받았는지 확인하기 위한 조사가 필요할 수 있다.
- 따라서, 개인정보 침해 사고의 ‘인지 시점’의 기준은 개인정보의 침해로 이어진 보안 사고의 발생을 컨트롤러가 합리적인 수준에서 확신한 때로 본다. 또한, 침해 사고를 감지하고 처리하기 위한 내부 프로세스 수립이 필요하다.

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

GDPR 관련 규정	<ul style="list-style-type: none">■ 제33조(감독기구에 대한 개인정보 침해 통지)■ 제34조(정보주체에 대한 개인정보 침해 통지)■ 전문 제85항~제88항■ Guidelines on Personal data breach notification under Regulation 2016/679,(2017.10.3.), WP29(EDPB 승인)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제34조(개인정보 유출 통지 등)



개인정보 침해 통지



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



셀프 체크리스트

Self Check List

	예	아니오
• 침해 사고인지 후 72시간 이내 감독 기구에게 통지하기 위한 프로세스를 구축하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 개인정보 침해 사고가 개인정보의 손실 혹은 유출만을 의미하지 않는다는 것을 이해하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.1.1 통지 의무

- 정보주체의 권리와 자유에 위협⁷³을 일으킬 가능성이 있는 침해가 발생할 경우 감독기구에 통지하여야 한다(제33조).

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

73 이에 대한 판단 기준은 [더 알아보기 8]를 참조

감독기구 통지 대상 판단 예시 : 가용성의 손실

- ▶ 일시적인 개인정보 가용성 손실은 보안 사고는 확실하나 정보주체의 권리와 자유에 위험을 발생시키는 경우에만 통지 대상이며, 사안별 판단 필요
 - ※ 병원에서 일시적으로 환자의 중요 의료 정보에 접근할 수 없음 → 수술 취소 등 개인의 권리와 자유에 대한 위험 발생 가능 → 통지 대상에 해당
 - ※ 언론사 시스템이 정전 등으로 수 시간 중단되어 독자 대상 뉴스레터 발송 불가 → 개인의 권리와 자유에 대한 위험 발생하는 경우가 아님 → 통지 대상 미해당
- ▶ 가용성의 일시적 손실로 개인에 대한 영향이 발생하지 않았더라도 통지가 요구될 수 있음에 주의할 필요가 있으며 침해의 모든 가능한 결과를 고려하는 것이 중요
 - ※ 랜섬웨어 감염 : 데이터 복구 전까지 일시적 가용성 손실 발생
 - ※ 외부 공격자에 의한 네트워크 침입 및 기밀성 침해(개인정보 접근)로 인해 개인의 권리와 자유에 위험이 발생한 경우 통지가 요구될 수 있음

2.1.2 통지 내용

- 개인정보 침해 내용을 통지할 때는 최소한 다음 내용을 포함하여야 한다.
 - ① 가능한 경우 침해로 인해 영향을 받는 정보주체의 범주(categories)⁷⁴, 개인정보 기록의 범주⁷⁵, 대략적인 개수를 포함한 개인정보 침해의 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 부당한 지체 없이(without undue delay) 72시간 이내에 관련 감독기관에 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).

74 정보주체 범주의 예시 : 아동(child) 및 기타 취약 그룹(other vulnerable groups), 장애인(people with disabilities), 정직원(employees) 또는 고객(customers) 등

75 개인정보 기록 범주의 예시 : 건강 정보(health data), 학력 기록(educational records), 사회 복지 정보(social care information), 재무 기록(financial details), 은행 계좌 번호(bank account numbers), 여권 번호(passport numbers) 등 정직원(employees) 또는 고객(customers) 등

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.

※ 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 부당한 지체 없이(without undue delay) 컨트롤러에게 통지하여야 한다.

2.1.6 문서화 의무

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

2.2 정보주체에 대한 통지 의무



셀프 체크리스트

Self Check List

	예	아니오
• 정보주체 대상 통지 항목과 절차에 대한 내부 체계를 수립하고 이를 정책에 반영하였는가?	<input type="checkbox"/>	<input type="checkbox"/>
• 정보주체가 스스로를 보호할 수 있도록 지원해야 한다는 점을 인지하고 있는가?	<input type="checkbox"/>	<input type="checkbox"/>

2.2.1 통지 의무

- 불필요한 통지에 따른 피로가 있을 수 있으므로 모든 침해에 대해 정보주체에게 통지할 필요는 없다. 컨트롤러는 개인정보의 침해가 개인의 권리와 자유에 대하여 높은 위험을 초래할 가능성이 있는 경우에 한해 정보주체에게 통지해야 한다(제34조). 이는 정보주체가 필요한 예방 조치(necessary precautions)를 취하여 침해 사고로부터 스스로를 보호하도록 지원하기 위함이다.

2.2.2 통지 내용

- 정보주체에게 통지할 때는 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 부당한 지체 없이(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.
- 이와 같은 경우 공공 통신 또는 유사한 방법을 통해 그와 동등한 효과적인 방식으로 통지해야 한다(제34조(3)(c)).

⇒ 사례 1

병원에서 침해사고가 발생했으며 환자의 기록이 공개되었다. 공개된 정보는 민감정보이며 제3자에게 알려졌기 때문에 정보주체에 상당한 영향을 미칠 가능성이 높다. 개인의 자유와 권리에 높은 위험을 초래할 가능성이 크기 때문에 정보 주체에 침해사실에 대해 통지하여야 한다.

⇒ 사례 2

대학교에서 직원이 사고로 졸업생 연락처 정보 기록을 지워버리는 침해사건이 발생했다. 이 정보는 백업으로 다시 생성되었다. 이 경우 개인의 자유와 권리에 높은 위험을 초래할 가능성이 낮기 때문에 정보주체에 통지할 필요가 없다.

2.3 위반 시 과징금

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

⇒ 과징금 부과 사례

- ▶ 헝가리 모 정당이 보유한 6,000명의 개인정보 DB가 외부 해커의 취약점 공격으로 인해 웹상에 노출되었음에도 동 사실에 대해 감독기구 신고, 정보주체 통지, 처리 사실을 기록 의무 등을 이행하지 않음 : GDPR 제33조(1), 제33조(5), 제34조(1) 위반 → 34,375유로 과징금 부과(2019. 04.)
- ▶ 헝가리의 컨트롤러가 개인정보 저장 플래쉬 메모리 분실 사실을 감독기구에 신고하지 않음 : GDPR 제33조 위반 → 15,150유로 과징금 부과(2019. 06.)
- ▶ 리투아니아의 은행의 웹사이트가 다른 은행과 공유되어 고객 약 9,000명의 지불 정보가 조회 가능한 상태였으나 동 사실을 감독기구에 신고하지 않음 → 61,500유로 과징금 부과(2019. 05.)

GDPR 관련 규정

- 제33조(감독기구에 대한 개인정보 침해 통지)
- 제34조(정보주체에 대한 개인정보 침해 통지)
- 전문 제85항~제88항
- Guidelines on Personal data breach notification under Regulation 2016/679, WP29

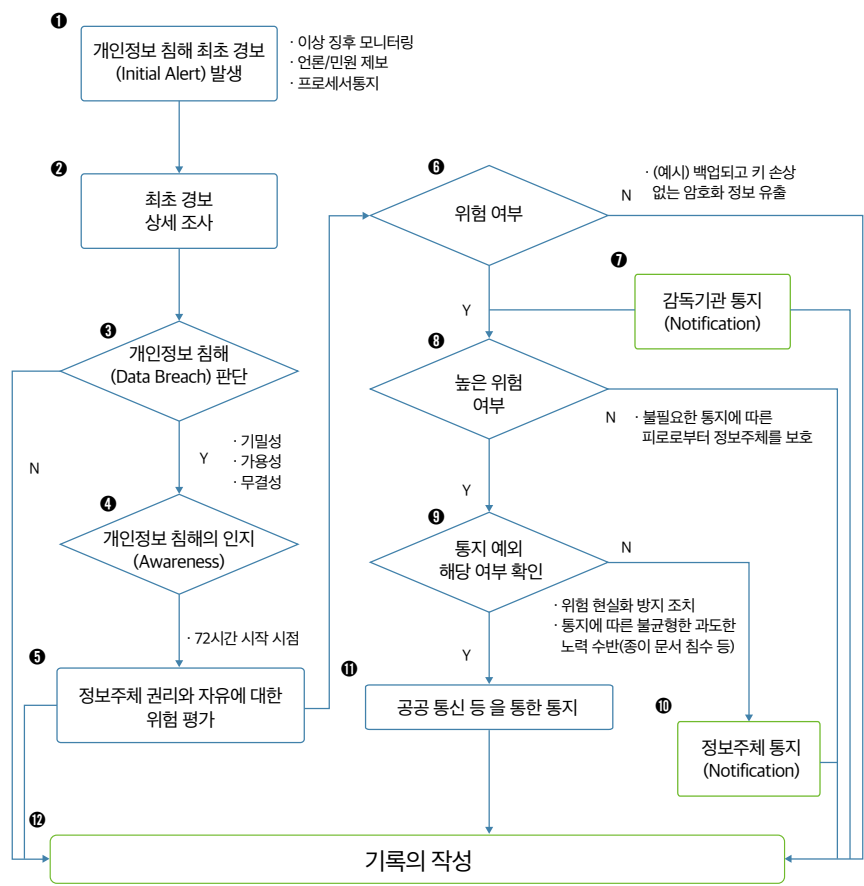
한국 개인정보보호법 관련 규정

- 제34조(개인정보 유출 통지 등)

+ 더 알아보기 / 8

개인정보 침해 통지 흐름도⁷⁶

| 그림 8. 개인정보 침해 통지 흐름도



76 제29조 작업반, Guidelines on Personal data breach notification., 2018. 02. 06.

#1 보안사고 감지/인지 및 개인정보 침해(personal data breach) 발생 여부 판단([그림 8]의 ①~③)

컨트롤러는 개인정보 침해 발생 여부를 즉시 파악하고, 감독기구 및 정보주체에게 통지할 수 있는 모든 적절한 기술적·관리적 보호조치 대책을 수립하여야 한다. 그 위험성에 대한 평가는 개인정보 침해가 발생되었다고 밝혀진 후에 이어지게 된다.

#2 개인정보 침해 인지 및 위험에 대한 평가([그림 8]의 ④~⑤)

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

#3 개인의 자유와 권리에 대한 위험을 초래할 가능성에 대한 평가([그림 8]의 ⑥~⑦)

개인정보 침해가 발생하는 경우 컨트롤러는 이를 인지한 때로부터 72시간 내 가능한 신속하게 관할 감독기구(주 감독기구)에게 통지하여야 한다. 다만, 이는 개인정보 침해가 개인의 권리와 자유에 대하여 위험을 초래할 가능성이 있는 경우에 해당한다. 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 포함된다. 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 있다.

| 표 10. 개인정보 침해에 대한 감독기구 통지 필요 여부 판단 예시

통지 필요 여부	예시
통지 불필요	<ul style="list-style-type: none">- 암호화된 개인정보가 유출되었을 때 암호 키의 기밀성이 손상되지 않은 경우 해당 정보는 원칙적으로 파악이 불가능함에 따라 개인에 대한 부정적인 영향을 미칠 가능성이 없으므로 통지 불필요- 비인가자가 해독할 수 없는 방식으로 개인정보가 만들어지고, 정보가 사본이거나 백업이 존재하는 경우, 올바른 방식으로 암호화 된 개인정보의 기밀성 침해는 감독기구에 통지 불필요- 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
통지 필요	<ul style="list-style-type: none">- 개인정보가 암호화된 경우에도 컨트롤러가 적절한 백업을 하지 않아 손실 또는 변경에 따른 부정적인 영향을 정보주체에게 발생시킬 수 있는 경우 통지 필요- 암호화된 개인정보가 유출되어 통지를 하지 않았으나, 시간이 지남에 따라 키가 훼손된 것으로 확인되거나 암호화 소프트웨어의 취약성이 노출된 경우 통지 필요- 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- 병원에서 일시적으로라도 환자의 중요 의료 정보에 접근할 수 없는 경우 수술 취소 등 개인의 권리와 자유에 대한 위험을 발생시킬 수 있으므로 통지 필요- 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

#4 개인의 권리와 자유에 높은 위험을 초래할 가능성에 대한 평가 및 정보주체 통지 ([그림 8]의 ③, ⑩)

개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우 영향을 받는 개인에게 통지하고 보호조치에 대한 정보를 제공하여야 한다. 높은 위험에 대한 판단 여부는 개인정보의 성격, 민감도, 개인 식별의 용이성, 개인에게 미치는 영향의 심각도, 개인의 특성, 영향 받는 개인의 수, 컨트롤러의 특성 등을 종합적으로 고려하여야 한다.

컨트롤러는 통지가 지연 없이 이루어졌다는 사실을 입증하여야 하며, 통지가 수행되지 않은 경우 과징금 부과 등 감독기구의 개입이 가능하다.

| 표 11. 개인정보 침해에 대한 정보주체 통지 불필요 예시

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

#5 통지 예외 해당 여부 확인 및 통지 대체 방안 확인([그림 8]의 ⑨, ⑪)

정보주체 대상 통지 예외 대상에 해당되는지를 확인하고 정보주체 대상 통지가 어려운 경우 공공 통신 또는 유사한 방법을 통해 그와 동등한 효과적인 방식으로 통지를 제공해야 한다(제34조(3)(c)).

#6 제33조제5항에 따른 문서화 및 기록 유지([그림 8]의 ⑫)

컨트롤러는 모든 침해 기록과 대응 조치 등에 대한 사항을 문서화하고 기록을 유지하여야 한다. 이는 감독기구 및 정보주체에 대한 통지 의무와는 관계없이 내부 관리 대장을 통하여 작성되도록 권고된다.

A large blue circle containing the white number '07'. Below the number is a horizontal yellow line.

07

피해구제 및
제재



1. 구제수단(Remedies)(제77~79조)
2. 손해배상청구권 및 책임
(Right to compensation and liability)(제82조)
3. 과징금(Administrative fines)(제83조)
4. 벌칙(Penalties)(제84조)



구제수단



Point

- 권리가 침해되었을 때 정보주체가 선택할 수 있는 피해 구제 수단들(제77조~제79조)을 이해할 수 있다.

1.1 감독기구에 민원을 제기할 권리

- 모든 정보주체는 기존의 행정적·사법적 구제를 받을 권리를 제한 또는 침해받지 않고 감독기구에 민원을 제기할 권리(right to lodge a complaint with a supervisory authority)(제77조)가 있다.
- 이 경우 정보주체는 거주지(habitual residence)나 근무지 또는 침해 발생이 있을 것으로 추정되는 장소가 소재한 회원국의 감독기구에 민원을 제기할 수 있다.
- 민원을 접수한 감독기구는 민원 처리 경과 및 결과를 사법적 구제 수단의 가능성과 함께 민원인에게 알려 주어야 한다.

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

1.2 감독기구의 결정에 관한 사법적 구제 수단

- 각 개인 또는 법인은 기존의 행정적 또는 비사법적 구제 수단을 제한받거나 침해받지 않고 감독기구의 법적 구속력 있는 결정에 대하여 효과적인 사법적 구제 수단에 관한 권리(judicial remedies against decisions of supervisory authorities)(제78조)를 가진다.
- 또한 정보주체는 감독기구가 민원을 처리하지 않거나, 제77조에 따른 민원 제기 후 3개

월 안에 민원 처리 경과 및 결과를 정보주체에게 알리지 않을 경우 효과적인 사법적 구제 수단에 관한 권리를 가진다.

- 이외에도 전문 제143항은 컨트롤러, 프로세서 또는 민원인이 EDPB의 결정에 대해 법원에 소송을 제기하고자 하는 경우 공표일로부터 2개월 이내에 할 수 있다고 설명하고 있다.

1.3 컨트롤러 또는 프로세서에 대한 효과적인 사법적 구제 수단에 관한 권리

- GDPR에서 정한 규정을 위반한 개인정보의 처리로 인해 자신의 권리가 침해된 것으로 판단한 정보주체는 위반 책임이 있는 컨트롤러나 프로세서를 상대로 효과적인 사법적 구제 수단에 관한 권리(right to an effective judicial remedy against a controller or processor)(제79조)를 가진다.
- 기존 Directive에서는 컨트롤러에 대해서만 사법 구제권을 요청할 수 있었던 반면, GDPR에서는 프로세서에 대해서까지 가능하다는 점에서 정보주체의 권리가 강화되었다고 볼 수 있다.
- 컨트롤러 또는 프로세서를 상대로 한 법적 절차는 해당 컨트롤러 또는 프로세서의 사업장(establishment)이 있는 회원국의 법정에서 진행되어야 한다. 대안으로, 컨트롤러 또는 프로세서가 공적 권한을 행사하는 회원국의 공공기관이 아니라면, 정보주체의 거주지가 있는 회원국의 법원에서 진행될 수 있다.

GDPR 관련 규정	<ul style="list-style-type: none">■ 제77조(감독기구에 민원을 제기할 권리)■ 제78조(감독기구에 대한 사법적 구제 수단)■ 제79조(컨트롤러 또는 프로세서에 대한 효과적인 사법 구제 수단)
한국 개인정보보호법 관련 규정	<ul style="list-style-type: none">■ 제62조(침해 사실의 신고 등)



손해배상청구권 및 책임



Point

- 컨트롤러와 프로세서의 손해배상 의무를 이해할 수 있다(제82조).

2.1 컨트롤러와 프로세서의 손해배상 의무

- GDPR 규정 위반으로 물질적 또는 비물질적 손해를 입은 자는 누구든지 컨트롤러 또는 프로세서에게 손해배상을 받을 권리(right to compensation and liability)(제82조)가 있다.
- 이를 구체적으로 살펴보면 다음과 같다.

① 컨트롤러는 위법한 개인정보 처리로 인해 발생한 손해에 대하여 책임을 부담한다.

※ GDPR은 금전 및 비금전 손해에 대해서도 명시적으로 배상받을 수 있다고 정하고 있다는 점에서 금전적인 손해에 대한 배상만 언급하고 있는 Directive와 차이가 있다.

② 프로세서는 GDPR에서 프로세서에 관하여 구체적으로 명시하고 있는 개인정보처리와 관련한 의무의 위반 또는 컨트롤러의 적법한 지시를 벗어나거나 이에 반하는 개인정보의 처리로 인해 발생한 손해에 대하여 책임을 부담한다.

③ 복수의 컨트롤러 또는 프로세서가 동일한(하나의) 개인정보 처리에 관여하여 손해가 발생한 경우, 각각의 컨트롤러 또는 프로세서는 정보주체의 효과적인 손해배상을 담보하기 위하여 발생한 전체 손해(entire damage)에 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 프로세서에 대한 구체적인 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 손해 발생과 관련된 사건에 대하여 책임이 없음을 증명하면 해당 책임으로부터 면제된다.

GDPR 관련 규정	■ 제82조(손해배상청구권 및 책임)
한국 개인정보보호법 관련 규정	■ 제39조(손해배상 책임)



과징금



Point

- 과징금 부과 및 가액의 원칙을 이해할 수 있다(제83조).
- 과징금 부과와 구체적 사례들을 이해할 수 있다.

3.1 원칙

- 과징금(administrative fines)은 자동으로 적용되지 않으며, 개별 사례별(each individual case)로 부과된다.

※ GDPR은 금전 및 비금전 손해에 대해서도 명시적으로 배상받을 수 있다고 정하고 있다는 점에서 금전적인 손해에 대한 배상만 언급하고 있는 Directive와 차이가 있다.

- 과징금의 부과는 효과적이고 비례적이며 억제력(dissuasive)이 있어야 한다.
컨트롤러 또는 프로세서의 동일하거나 관련된 개인정보의 처리가 GDPR의 여러 규정을 위반하는 경우, 과징금은 가장 중한 침해와 관련한 금액을 초과할 수 없다.

3.2 최대 과징금

3.2.1. 전 세계 연간 매출액 4% 또는 2천만 유로 중 더 큰 금액을 상한으로 하는 과징금

- 아래의 GDPR 규정을 위반하는 경우 직전 회계연도 전 세계 매출액의 4% 또는 2천만 유로 중 더 큰 금액을 한도로 과징금이 부과된다.
 - ① 개인정보 처리의 기본 원칙(제5조), 합법처리의 원칙(제6조), 동의의 조건에 관한 규정(제7조) 및 민감정보 처리에 관한 규정(제9조)
 - ② 정보주체의 권리에 관한 제12조부터 제22조까지
 - ③ 제3국이나 국제기구의 수령인에게로 개인정보를 이전할 때 준수해야 하는 제44조부터 제49조의 규정
 - ④ 제9장에서 정한 바에 따라 채택된 회원국 법률에 따른 의무에 관한 규정

- ⑤ 제58조 제2항에 따라 감독기구가 내린 명령 또는 정보 처리의 임시적 또는 확정적 제한 (temporary or definitive limitation)을 위반하는 경우, 또는 개인정보 이동 중지 명령을 준수하지 않거나 감독기구의 접근을 허용하지 않아 제58조 제1항을 위반한 경우

3.2.2 전 세계 연간 매출액 2% 또는 1천만 유로 중 더 큰 금액을 상한으로 하는 과징금

- 아래의 GDPR 규정을 위반한 경우에는 1천만 유로 또는 직전 회계연도의 연간 전 세계 총 매출의 2%에 이르는 과징금 중 더 큰 금액을 한도로 과징금이 부과된다.
 - ① 컨트롤러, 프로세서의 의무와 관련한 제8조, 제11조, 제25부터 39조, 제42조, 제43조
 - ② 인증기관의 의무에 관한 제42조 및 제43조
 - ③ 행동규약 준수 모니터링의 의무에 관한 제41조제4항
- 참고로, 2018년 5월 25일 GDPR 시행 이후 주요 국가들의 주요 과징금 부과 사례들을 표로 정리하면 아래와 같다.⁷⁷

| 표 12. 주요 과징금 부과 사례

발표일자 국가	과징금 액수	과징금 부과 의지	관련 GDPR 규정
2018. 09. 12. 오스트리아 (최초의 과징금 부과 사례)	약 €5,280	스포츠 베팅 카페가 설치한 CCTV 카메라가 주변 보행자를 촬영하도록 한 행위가 개인정보 처리 목적에 부합하지 않으며 처리되는 개인정보를 필요최소한으로 제한하지 않는다는 이유 등으로 부과	제5조, 제6조 등
2019. 01. 21. 프랑스	약 €5,000만	구글이 개인정보 처리방침에 투명하고 이해하기 쉬운 방식으로 관련정보를 게시하지 않은 행위, 광고 개인화를 목적으로 하는 개인정보 수집에 대한 동의를 구체적이고 명료하게 받지 않은 행위 등에 대하여 부과	제4조부터 제6조, 제13조, 제14조
2019. 07. 08. 영국	약£ 1억 8,300만	영국 항공(British Airways)의 고객 500,000명의 개인정보가 허위 인터넷 사이트를 통해 유출되는 사고와 관련하여, 충분한 보호 조치를 취하지 않았다는 이유로 부과	제32조
2019. 07. 09. 영국	약 £9,920만	메리어트의 고객 3억 3,900만명의 개인정보가 유출되는 사고와 관련하여, 메리어트의 스타우드 인수 당시 충분한 실사(due diligence) 및 보호조치를 취하지 않았다는 이유로 부과	제32조
2019. 10. 23. 오스트리아	약 €1,800만	오스트리아 우체국이 300만 명 이상의 주소, 개인적 선호 등에 대한 프로필을 생성하여 이를 정당, 회사 등에 판매한 행위에 대하여, 개인정보 처리에 대한 근거가 없다는 이유로 부과	제5조, 제6조

77 GDPR 과징금 부과 관련 최신 사례들에 관한 정보는 GDPR Enforcement Tracker(<http://www.enforcementtracker.com>) 참조

2019. 10. 30. 독일	약 €1,450만	부동산 회사가 거주자들에 대한 개인정보를 필요 여부와는 무관하게 장기간 보관한 행위에 대하여, 개인정보 처리원칙을 위반하였다는 이유로 부과	제5조, 제25조
2020. 01. 15. 이탈리아	약 €2,780만	이탈리아 주요 이동통신사인 TIM사가 소비자 동의없이 홍보 및 영업활동을 전개하고 어플리케이션 내 이용자 동의 획득과정이 개인정보 처리에 대한 합법처리근거를 위반하였다는 이유로 부과	
2020.10.01. 독일	약 €3,526만	패션업체 H&M의 독일법인은 직원의 건강정보 등 민감 정보와 휴가 등 사생활 관련 정보를 동의 없이 은밀히 수집해 개인정보 동의와 처리 규정을 위반	제5조, 제6조
2021.01.08. 독일	€1,040만	독일 전자제품 소핑몰 Notebooksbilliger는 직원과 고객들의 사전 동의 없이 CCTV를 통해 이들을 감시했으며, 장기간 해당 정보를 저장한 것과 관련해 동의 규정 위반 및 삭제/저장 기한 규정 위반을 이유로 부과	제5조, 제6조
2021.07.16. (추정) 룩셈부르크	약 €7억 4,600만	다수의 주요 언론매체가 아마존의 미국 증권거래소 재무 실적 제출 자료를 근거로 아마존 유럽 본사에 대해 룩셈부르크 개인정보 감독기구가 과징금을 부과한 것으로 추정. 공식적인 발표는 없는 가운데 위반 내용은 고객의 동의가 없는 상업적 광고에 관한 것으로 추정. 해당 과징금 규모는 역대 최대	제6조, 제7조
2021.09.02. 아일랜드	€2억 2,500만	메타플랫폼의 메신저 앱 왓츠앱은 사용자들로부터 획득한 개인정보의 저장, 목적, 처리 방침에서 투명성 원칙 위반	제5조, 제12조, 제23조, 제14조
2022.02.10. 이탈리아	€2,000만	미국계 인공지능 기술 기반 안면 인식 분석 업체 클리어뷰 AI는 전 세계 소셜미디어 등 웹 소스로부터 획득한 100억 개 이상의 사진을 통해 사람들로부터 동의를 받지 않은 안면 정보를 수집해 프로파일링을 수행. 이와 관련해 사전 동의 원칙, 목적 제한의 원칙, 저장 제한의 원칙 등 위반 ※ 동 건과 유사 건으로 클리어뷰 AI에 대해 그리스(22.7월), 프랑스(22.10월)도 각각 2,000만 유로의 과징금 부과	제5조, 제9조, 제12조, 제13조, 제14조, 제15조
2022.03.15. 아일랜드	€1,700만	페이스북(현 메타플랫폼)은 개인정보 보안 규정과 침해 사고 후 보고 규정을 위반	제5조, 제24조, 제32조
2022.05.18. 스페인	€1,000만	구글이 삭제를 요청한 개인정보를 충분한 법적 근거 없이 제3자인 루멘 프로젝트와 공유한 행위에 대해 부과	제6조, 제17조
2022.09.05. 아일랜드	€4억 500만	메타플랫폼 계열 인스타그램에서 아동이 개인 계정이 아닌 기업 계정을 사용할 경우 전화번호, 이메일 등이 자동으로 노출되는 것 등과 관련해 아동 개인정보보호 규정 위반을 이유로 부과	제5조, 제6조, 제12조, 제24조, 제25조

GDPR 관련 규정

■ 제83조(과징금 부과에 관한 일반 조건)

한국 개인정보보호법 관련 규정

■ 제34조의2(과징금의 부과 등)



- 개별 EU 회원국의 법률상 차이로 인해 서로 다른 수준의 벌칙(penalties)이 존재한다.
- 개별 EU 회원국은 GDPR에 따라 각국 법률에 반영하는 조치를 2018년 5월 25일까지 EU 집행위원회에 알리고, 해당 법률에 영향을 미치는 차후의 개정사항을 지체 없이 (without delay) 집행위원회에 통보하여야 한다.

GDPR 관련 규정	■ 제84조(벌칙)
한국 개인정보보호법 관련 규정	■ 제9장(벌칙)

+ 더 알아보기 / 9

과징금 부과 및 가액 평가 기준

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

#1 위반 행위의 성격, 심각성 및 지속 기간

위반 행위의 성격

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

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

위반 행위의 심각성 및 지속 기간

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

① 정보주체의 수

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

② 목적

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

③ 피해 수준

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

④ 지속 기간

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

#2 위반의 의도성 또는 태만

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

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

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 해당된다.

#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 한다.

※ 예 : 데이터 처리와 관련된 다른 컨트롤러·프로세서에게 통지, 이미 발생한 것보다 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 있다.

#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 행위와의 관련성을 평가할 수 있다.

#6 위반 행위 개선을 위한 감독기구와의 협조

GDPR 제83조제2항은 과징금 부과 여부 및 과징금 가액 결정 시 컨트롤러·프로세서의 감독기구와의 협조 수준에 따라 상당한 고려가 이루어질 수 있다고 규정하고 있다.

#7 위반으로 인해 영향을 받게 되는 개인정보의 종류

위반 행위를 통하여 영향을 받는 개인정보가 다음에 해당하는지 여부에 따라 과징금 가액 결정은 상이할 수 있다. 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·관리적 보호조치가 적용된 경우

#8 감독기구에 위반 행위 발생 사실 통지 여부

컨트롤러의 위반 행위에 대한 감독기구 통지는 법적 의무이므로 그 이행 여부에 따라 처벌 수준이 경감될 수는 없다. 다만 그 의무를 미이행한 컨트롤러·프로세서 는 보다 중대한 제재 대상으로 판단될 수 있다.

#9 과거 동일한 사안에 대한 감독기구의 시정 조치 내역

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

#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 있다. 이때 컨트롤러와 프로세서는 모니터링 기구에 의해 행동규약의 준수 여부가 감시되며, 준수 여부 역시 위반 행위의 평가에 있어 참조 기준이 될 수 있다.

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

위반 행위를 통하여 얻은 이익에 대한 정보는 과징금 부과에 강력한 근거가 될 수 있다. 따라서 기업이 위반 행위를 통하여 얻은 직·간접적 이익이나 회피한 손실 등을 검토할 수 있다.

+ 더 알아보기 / 10

GDPR의 제재 규정

제재 종류	주요내용	관련조문
손해배상 (제82조)	<ul style="list-style-type: none"> GDPR 위반의 결과로 물질적 또는 비물질적 손해를 입은 정보주체는 그 손해에 대하여 컨트롤러나 프로세서로부터 배상을 받을 수 있다. 	-
	<ul style="list-style-type: none"> 컨트롤러는 GDPR을 위반하는 처리가 일으킨 손해에 대하여 책임을 지야 한다. 다만 손해를 일으킨 사건에 대하여 책임이 없음을 입증하면, 컨트롤러 또는 프로세서의 책임면제가 가능하다. 	
	<ul style="list-style-type: none"> 복수의 컨트롤러 또는 프로세서가 일으킨 손해에 대하여 책임이 있는 경우 정보주체의 실효적 배상을 위하여 모든 손해에 대한 책임을 부담한다. 이 경우 하나의 컨트롤러나 프로세서가 완전한 배상을 하면 다른 컨트롤러나 프로세서에 대한 구상권 행사가 가능하다. 	
과징금 (제83조)	<ul style="list-style-type: none"> EU 회원국 감독기구는 과징금 부과권이 있다. 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. 	-
	전 세계 연간매출액 2% 또는 1천만유로 중 더 큰 금액부과	
	<ul style="list-style-type: none"> 컨트롤러 및 프로세서 의무위반 	제8조, 제11조, 제25조~제39조, 제42조, 제43조
과징금 (제83조)	<ul style="list-style-type: none"> 인증기관 의무위반 	제42조, 제43조
	<ul style="list-style-type: none"> 공인된 행동규약 준수에 대한 모니터링 의무위반 	제41조제4항
과징금 (제83조)	전 세계 연간매출액 4% 또는 2천만 유로 중 더 큰 금액부과	
	<ul style="list-style-type: none"> 동의의 조건을 포함하여 개인정보 처리 기본원칙 위반 	제5조~제7조, 제9조
	<ul style="list-style-type: none"> 정보 주체의 권리보장 의무위반 	제12조~제22조
	<ul style="list-style-type: none"> 제3국이나 국제기구의 수령인에게 개인정보 이전 시 준수 의무 위반 	제44조~제49조
	<ul style="list-style-type: none"> 제24조~제43조에 따라 채택된 EU 회원국 법률의무위반 	-
과징금 (제83조)	<ul style="list-style-type: none"> 감독기구가 내린 명령 또는 정보처리의 제한 불복 감독기구의 개인정보 이동 중지 명령 미준수 및 정보주체의 접근권 보장 의무위반 	제58조제2항 제58조제1항

제재 종류	주요내용	관련조문
벌칙 (제84조)	<ul style="list-style-type: none">• 회원국의 과징금이 부과되지 않는 위반에 대한 벌칙규정 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 통보하여야한다.	-



08

참고자료



1. GDPR 적용 대상 국가의 감독기구 현황
2. 주요 질의 및 답변(Q&A)
3. 사업자를 위한 EU 집행위원회의 7단계 체크리스트
4. ICO 컨트롤러-컨트롤러간 SCC
(표준 개인정보보호조항) 번역
5. 해외의 GDPR 관련 가이드 발간 현황
6. 원스톱숍 메커니즘



GDPR 적용 대상 국가의 감독기구 현황

▶ EU 국가별 감독기구 현황(2021년 12월 31일 현재)

■ 오스트리아(Austria)

Österreichische Datenschutzbehörde

Address: Barichgasse 40-42

1030 Wien

Tel. +43 1 52152 2550

email: dsb@dsb.gv.at

Website: <http://www.dsb.gv.at/>

Tel. + 359 2 91 53 519

email: kzld@cpdp.bg

Website: <https://www.cdpd.bg/>

■ 크로아티아(Croatia)

Croatian Personal Data Protection Agency

Address: Selska cesta 136 HR - 10 000 Zagreb

Tel. +385 1 4609 000

Fax +385 1 4609 099

email: azop@azop.hr

Website: <http://www.azop.hr/>

■ 벨기에(Belgium)

Autorite de la protection des donnees -

Gegevensbeschermingsautoriteit (APDGBA)

Address: Autorité de protection des données

Rue de la presse 35, 1000 Bruxelles

Tel. +32 2 274 48 00

Fax +32 2 274 48 35

email: dpo@apd-gba.be

Website: [https://www.](https://www.autoriteprotectiondonnees.be/)

autoriteprotectiondonnees.be/

■ 키프로스(Cyprus)

Office of the Commissioner for Personal Data
Protection

Address: 1 Iasonos Street,

1082 Nicosia

P.O. Box 23378, CY-1682 Nicosia

Tel. +357 22 818 456

Fax +357 22 304 565

email: commissioner@dataprotection.gov.cy

Website: <http://www.dataprotection.gov.cy/>

■ 불가리아(Bulgaria)

Commission for Personal Data Protection

Address: 2, Prof. Tsvetan Lazarov blvd.

Sofia 1592

Website: <http://www.uoou.cz/>

Website: <http://www.datatilsynet.dk/>

Website: <http://www.aki.ee/>

Website: <http://www.tietosuoja.fi/en/>

Website: <http://www.cnil.fr/>

Website: <http://www.bfdi.bund.de/>

Website: <http://www.dpa.gr/>

Budapest

Tel. +36 1 3911 400
email: ugyfelszolgalat@naih.hu
Website: <http://www.naih.hu/>

■ 아일랜드(Ireland)

Data Protection Commission
Address: 21 Fitzwilliam Square South Dublin
2, D02 RD28 Ireland
Tel. +353 1 76 50100
email: info@dataprotection.ie
Website: <http://www.dataprotection.ie/>

■ 이탈리아(Italy)

Garante per la protezione dei dati personali
Address: Piazza Venezia n. 11 - 00187 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 3785
email: protocol@gpdp.it
Website: <http://www.garanteprivacy.it/>

■ 라트비아(Latvia)

Datu valsts inspekcija
Address: Elijas iela 17 Rīga, LV-1050
Tel. +371 6722 3131
Fax +371 6722 3556
email: info@dvi.gov.lv
Website: <http://www.dvi.gov.lv/>

■ 리투아니아(Lithuania)

Valstybinė duomenų apsaugos inspekcija
Address: L. Sapiegos g. 17
LT-10312 Vilnius
Tel. +370 5 212 75 32

Fax +370 5 261 94 94
email: ada@ada.lt
Website: <https://vdai.lrv.lt/>

■ 룩셈부르크(Luxembourg)

Commission Nationale pour la Protection
des Données
Address: 1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
Tel. +352 2610 60 1
Fax +352 2610 60 99
email: info@cnpd.lu
Website: <http://www.cnpd.lu/>

■ 몰타(Malta)

Office of the Information and Data
Protection Commissioner
Address: Second Floor, Airways House
High Street, Sliema SLM 1549
Tel. +356 2328 7100
Fax +356 2328 7198
email: idpc.info@idpc.org.mt
Website: <http://www.idpc.org.mt/>

■ 네덜란드(Netherlands)

Autoriteit Persoonsgegevens
Address: Bezuidenhoutseweg 30
P.O. Box 93374
2509 AJ Den Haag/The Hague
Tel. +31 70 888 8500
Fax +31 70 888 8501
Website: <https://autoriteitpersoonsgegevens.nl/nl>

■ 스웨덴(Sweden)

Swedish Authority for Privacy

Protection(IMY)

Address: Drottninggatan 29

5th Floor

Box 8114

104 20 Stockholm

Tel. +46 8 657 6100

Fax +46 8 652 8652

email: imy@imy.se

Website: <http://www.imy.se/>

▶ 유럽 자유무역 연합(EUROPEAN FREE TRADE AREA)

■ 아이슬란드(Iceland)

Persónuvernd
Address: Rauðarárstígur 10
105 Reykjavík
Tel: +354 510 9600
email: postur@dpa.is
Website: <https://www.personuvernd.is> or
<https://www.dpa.is>

■ 리히텐슈타인(Liechtenstein)

Data Protection Office, Principality of
Liechtenstein
Address: Städtle 38
9490 Vaduz
Principality of Liechtenstein
Tel. +423 236 6090
email: info.dss@llv.li
Website: <https://www.datenschutzstelle.li>

■ 노르웨이(Norway)

Datatilsynet
Address: Tollbugata 3
0152 Oslo
Tel +47 22 39 69 00
email: postkasse@datatilsynet.no
Website: www.datatilsynet.no

■ 스위스(Switzerland)

Data Protection and Information
Commissioner of Switzerland
Address: Feldeggweg 1 3003 Bern
Tel. +41 58 462 43 95
Fax +41 58 462 99 96
email: contact20@edoeb.admin.ch
Website: <https://www.edoeb.admin.ch/>



주요 질의 및 답변(Q&A)

아래 질문과 답변은 EU 집행위원회에서 공개 게시한 FAQs와 한국인터넷진흥원 GDPR 대응 센터를 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 알려드립니다.

EU 집행위원회 질의응답 사례

Q1 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.

Q2 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)

Q3 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 제공하거나 EU 역내의 정보 주체를 모니터링하는 경우

예: ① GDPR 적용 경우: 교육 업체가 EU 내의 스페인어권과 포르투갈어권 대학에 강좌를 개설하고, 서비스 제공을 위하여 고객의 ID와 비밀번호를 요구하는 경우 ② GDPR 적용 예외 경우: EU 역외에 설립된 기업이 EU를 포함하는 다수 국가를 여행하는 EU 역외의 정보주체에게 서비스를 제공하는 경우로, EU 내 정보주체를 구체적으로 겨냥하지 않는 경우

Q4 컨트롤러(Controller)와 프로세서(Processor)란 무엇인가요?

A 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

Q5 개인정보 삭제권(잊힐 권리)이란 무엇인가요?

A 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 개인정보를 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 개인정보가 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)

Q6 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

Q7 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 - 쇼핑몰이나 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

Q8 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 민감정보를 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 신용정보를 활용하여 고객을 평가하는 경우
- 병원에서 환자의 건강정보를 포함하여 새로운 건강정보 데이터베이스를 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

Q9 개인정보를 역외 이전할 수 있는 조건은 무엇인가요?

A 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, BCR)
 - ② 표준 개인정보보호 조항(Standard data protection clauses)에 의거한 개인정보 이전 계약
 - ③ 승인된 행동규약(code of conduct) 및 인증제도(certification mechanism)
- 3) 특정상황에 대한 몇 가지 예외*에 해당되는 경우

* 정보주체가 적정성 승인이나 보호조치가 되어있지 않아 발생할 수 있는 위험성에 대해 고지 받은 후 명시적 동의를 한 경우 등

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 2)의 보호조치 중 하나를 채택한 경우 또는 특정상황에 대한 예외에 해당하는 경우 역외 이전이 가능

Q10

GDPR 위반에 따른 과징금의 부과 및 가액 원칙은 무엇인가요?

A

GDPR 위반의 경우 전 세계 매출액 2% 또는 1천만 유로 중 더 큰 금액이, 심각한 위반의 경우 전 세계 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

▶ GDPR 적용 범위

Q 암호화된 정보도 개인정보에 해당하나요?

- 암호화된 정보라 하더라도 추가적인 암호키를 이용하면 특정 정보주체에게 귀속될 수 있으므로, 암호화된 정보는 가명처리된 정보에 해당하고, 따라서 이는 개인정보에 해당합니다.
- 참고로, 익명처리된 정보는 이러한 식별가능성까지 모두 제거한 정보로서 이는 개인정보에 해당하지 **않고**, 따라서 GDPR이 적용되지 **않습니다**.

Q 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 EU시장을 염두에 두고 있을 때 적용됩니다. 이는 EU시장에서 통용되는 언어나 통화로 재화나 서비스를 직접적으로 제공하거나 그에 바탕을 두고 서비스를 제공함을 의미합니다.
- 영어를 사용하여 상품이나 서비스를 제공하고 있다는 것만으로는 그 컨트롤러나 프로세서가 하나 이상의 EU 회원국 내의 정보주체에게 서비스를 제공하는 것을 예상하고 있음이 명백하다고 볼 수 없습니다. 따라서 이것만으로는 GDPR이 적용되지 않습니다.
- 단, EU시장에 서비스를 제공하기 위한 명백한 목적을 바탕으로 개인정보를 수집·처리한다면 GDPR이 적용될 수 있습니다.

▶ 컨트롤러-프로세서

Q 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.

▶ DPO 임명

Q DPO 지정 후 감독당국에게 통보하거나 신고해야 하나요?

- GDPR 제37조제7항은 “컨트롤러 또는 프로세서는 DPO의 연락처를 공개하고 감독당국에 통지하여야 한다.”고 규정하고 있으므로, DPO를 지정한 후에는 그 연락처를 감독당국에 통지하여야 합니다.

Q DPO 임명 시 자격요건은 어떤 것이 있나요?(특정 자격을 취득해야 하는지?)

- GDPR 제37조제5항은 “DPO는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 제39조에서 언급된 직무를 수행할 능력에 근거하여 지정되어야 한다”고 규정하고 있습니다.
- 따라서 DPO가 되기 위한 별도의 자격증이 필요한 것은 아니고 반드시 내부 임직원이어야 할 필요도 없습니다. 다만 위와 같은 전문적 자질이 반드시 필요하며, 관련 자격증을 보유하고 있다면 그러한 자질이 있음을 입증하는 데에 도움이 될 수 있습니다.

Q 컨트롤러와 프로세서가 DPO를 따로 지정해야 하나요?

- GDPR 제37조는 DPO의 지정 의무는 컨트롤러 혹은 프로세서 해당 여부와 무관하게 적용됩니다. 즉 DPO 의무 지정사유에 누가 해당하느냐에 따라 어떤 경우에는 컨트롤러만, 어떤 경우에는 프로세서만, 혹은 양 측 모두가 DPO를 지정해야 하는 경우가 발생할 수 있습니다.

Q EU 내 법인이나 지사가 여러 곳이라면, 공동 DPO를 임명해도 되나요?

- GDPR 제37조제2항에 따라 사업체 집단은 각 사업장에서 “쉽게 접근이 가능 경우(easily accessible)”, 복수 사업자가 단일 DPO를 지정할 수 있습니다. 단, ‘사업체 집단(a group of undertakings)’에 해당하는 경우에만 가능하며, 사업적 관계가 없는 여러 독립 법인이 단일 DPO를 지정할 수는 없습니다.

▶ 개인정보 역외이전

Q 적정성 결정을 받으면 GDPR 준수 관련한 다른 조항들의 적용도 면제되나요?

- 적정성 결정은 개인정보의 역외이전에 대한 승인이므로, GDPR의 다른 규정이 적용 면제되는 것은 아닙니다. 따라서 정보주체의 권리 보장 및 DPO 임명, 처리활동 기록 등 자사에 적용되는 GDPR 조항들은 모두 준수해야 합니다.

Q SCC(표준 개인정보보호 조항)를 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

③ Decision 2010 / 87 / EU(and repealing Decision 2002 / 16 / EC)

〈컨트롤러에서 프로세서로 이전하는 경우〉

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

① 정보 수출자(Data exporter)와 정보 수입자(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 SCC의 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 SCC 조항은 EC 홈페이지에서 확인할 수 있습니다.https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Q 개인정보 역외이전에 대한 예외조항으로 명시적 동의란 무엇인가요?

- ‘명시적’이란 정보주체에 의해 동의를 표현되는 방식을 의미합니다. 이는 일반적인 동의에 비해 정보주체의 동의를 명확하게 확인될 수 있는 방식을 의미합니다. 구체적으로, 이메일에 동의 의사를 표시하여 제출하거나, 전자서명을 하는 방식, 동의에 대한 2단계 검증 등이 있습니다.

- 역외이전에 대한 유효한 명시적 동의 획득을 위해서는 보호조치가 갖추어지지 않

은 국가 혹은 기업으로 개인정보가 이전된다는 사실과 그 위험성에 대한 사전 고지가 있어야 합니다.

▶ 정보주체 권리

Q 정보주체가 제3자에게의 개인정보 이동을 요구하면 어떤 형식으로 그 파일을 전달해줘야 하고 전달해줘야 하는 파일의 범위는 어디까지인가요?

- 정보주체가 개인정보의 이동을 요구하는 경우, 컨트롤러 및 프로세서는 체계화되고 일반적으로 사용되며 컴퓨터로 해독이 가능한 형식으로 이를 전달해야 합니다.
- 단, 정보주체의 동의 또는 계약에 근거하여 처리되는 개인정보에 대해서만 이동권을 행사할 수 있으며, 컨트롤러 혹은 프로세서가 기존에 수집한 개인정보를 바탕으로 추론 및 재생산한 개인정보는 이동권의 대상에서 제외됩니다.

Q 프로파일링이 및 자동화된 개인정보 처리란 무엇을 의미하나요?

- ‘프로파일링’이란 자연인과 관련된 일정한 개인적 측면을 평가하기 위하여, 특히 그 자연인의 업무 능력, 경제 상황, 건강, 개인적 선호, 관심사, 신뢰도, 행동, 위치 또는 이동과 관련된 측면을 분석하거나 예측하기 위하여 개인정보를 사용하는 모든 형태의 자동화된 개인정보 처리를 의미합니다.
- ‘자동화된 개인정보 처리’란 인적 개입없이 기술적 수단에 의해서만 이루어지는 개인정보 처리를 의미합니다.

▶ 기업 책임성

Q 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?

- WP29에서 발간한 가이드라인에서 높은 위험을 초래할 가능성이 있는 개인정보 처리의 기준 9가지를 제시하고 있습니다.
 - 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 2개 이상 해당하는 처리작업은 영향평가가 필요하다고 할 수 있습니다.

▶ 동의

Q GDPR 시행 이전에 획득한 동의는 GDPR 시행 이후에도 유효한가요?

- GDPR 시행 이전에 획득한 동의라 하더라도 위와 같은 GDPR상 유효한 동의의 요건을 충족하고 있다면 시행 이후에도 유효합니다.

Q 성별과 IP, 각종 기기 식별자 및 위치 식별자 등 개인정보 수집 전체에 동의를 하여야만 사이트 이용이 가능하도록 하는 경우 GDPR 위반인가요?

- GDPR 제7조 제4항은 ‘동의를 자유롭게 이뤄졌는지를 판단할 때, 무엇보다도, 서비스 제공을 포함한 계약의 이행이 해당 계약 이행에 불필요한 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려하여야 한다’고 규정하고 있습니다.

- 따라서 사이트 이용에 불필요한 개인정보의 처리에 대한 동의를 조건으로 사이트를 이용할 수 있게 하는 경우 그러한 동의는 위 조건을 충족하지 못하여 GDPR 위반에 해당합니다.

▶ 영국의 EU 탈퇴와 GDPR

Q EU를 탈퇴한 영국도 GDPR에 따른 개인정보 역외이전 규정을 준수하여야 하나요?

- 영국은 EU를 탈퇴하였기 때문에 원칙적으로는 역외이전 규정을 준수해야 합니다

- 그렇지만 2021년 2월 EU 집행위원회가 영국 개인정보보호 법제에 대해 적정성 결정을 내리고 6월 최종 발표함에 따라, GDPR 체제 아래 EU 시민의 영국으로의 개인정보 역외이전이 가능해졌습니다.



사업자를 위한 EU 집행위원회의 7단계 체크리스트⁷⁸

이 가이드는 GDPR에 대응하기 위해 중소기업 등이 짚고 넘어가야 할 7가지 단계의 체크리스트에 대해 기술하고 있습니다.

✓ STEP ▶ 01

check ☐

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 ▶ 02

check ☐

개인정보 수집 시 고객 및 직원 등 관련된 각 개인에게 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

⁷⁸ European Commission, Seven steps for businesses to get ready for the General Data Protection Regulation, 2018.

개인정보를 접근할 수 있도록 해야 하고, 이 때 요청 정보를 가능한 한 신속하게 제공할 수 있도록 분류·보관하는 것이 권장됩니다.

✓ STEP 03

check ☐

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 04

check ☐

처리하는 개인정보에 대하여 보호조치를 수립하였습니까?

IT 시스템에 개인정보를 보관하는 경우, 비밀번호 설정 등을 통하여 접근을 제한하여야 합니다. 또한 이용하는 시스템의 보호조치가 정기적으로 최신성을 유지할 수 있도록 하여야합니다. 만약 개인정보를 물리적으로 보관하는 경우에는 비인가된 접근을 차단하고 안전한 장소에 보관하여야 합니다.

✓ STEP 05

check ☐

개인정보 처리 활동을 문서화하여 보관하고 있습니까?

처리하는 개인정보의 특성과 목적 등을 기록하여야 합니다. 감독기구의 요청에 적당하게 개인정보 처리를 기록할 필요가 있습니다. 문서화하여 기록하여야 하는 목록은 다음사항을 포함합니다.

- ① 개인정보 처리의 목적

- ② 개인정보의 유형
- ③ 정보주체의 유형⁷⁹
- ④ 수령인의 유형⁸⁰
- ⑤ 개인정보 보유기간
- ⑥ 개인정보 보호를 위한 기술적·관리적 보호조치
- ⑦ 개인정보가 EU 역외로 이전되는지 여부

✓ STEP ▶ 06

check ☐

하청계약 업체의 GDPR 준수 여부를 모니터링하고 있습니까?

만약 아웃소싱 등 외부 업체를 통하여 개인정보를 처리한다면 GDPR 준수를 입증할 수 있는 업체를 선정하여야 합니다. 외부 업체와 계약을 체결하기 이전에 GDPR 준수 여부를 확인하고, 이에 대해 계약서에 명시할 수 있습니다.

✓ STEP ▶ 07

check ☐

기업의 책임성 강화를 위한 다음 조항들을 검토하고 있습니까?

- ① 보다 안전한 개인정보보호를 위하여 DPO를 지정하고 있습니까? 단, 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? 공공장소에서 의 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 알려 드립니다.



영국의 EU탈퇴(Brexit)와 개인정보보호

(개요) 영국은 2016년 6월 국민투표에서 영국의 EU탈퇴를 확정하고, 2020년 1월 31일부로 정식 탈퇴하였습니다. 영국은 EU 탈퇴로 인한 법적 공백을 메우기 위해 2018년 EU탈퇴법(European Union (Withdrawal) Act 2018)을 제정하여 영국에 직접 적용해오던 EU의 법령을 그대로 영국의 국내법으로 계승한다고 규정하였습니다. 그러나 영국은 향후 점진적으로 EU와 다른 자국의 법적 체계를 정비해 나갈 것입니다.

(개인정보보호 관련 법) 영국에서는 헌법에서 개인의 프라이버시를 보호하고 있으며, 관련 주요 법으로는 ▲UK GDPR ▲개인정보보호법(Data Protection Act 2018, DPA 2018) ▲프라이버시 전 자통신 규정(Privacy and Electronic Communications Regulation 2003, PECR) 등이 있습니다.

- (UK GDPR) 영국은 EU GDPR의 내용을 거의 그대로 유지하고 일부 조문이나 단어를 대체, 추가, 제거한 UK GDPR을 2021년 1월에 발효해 개인정보보호와 관련된 큰 틀을 마련했습니다.

- (개인정보보호법 2018, DPA 2018) 동 법은 개인정보보호와 관련해 최초 1984년 제정되었으며 2018년 EU GDPR 시행에 맞추어 큰 폭으로 개정·발효되었습니다. DPA 2018은 GDPR이 영국 현실에 비추어 미치지 못하거나 반영하지 못하는 내용을 주로 담고 있습니다. 동 법은 총 7장 215 개 조항으로 이루어져 있으며 ▲UK GDPR 등에 따른 개인정보 처리(제2장) ▲사법 당국의 법 집행을 위한 개인정보 처리(제3장) ▲국가 정보기관(Intelligence services)에 의한 개인정보 처리(제4장) ▲정보커미셔너(ICO 커미셔너)의 역할(제5장) ▲법 집행절차(제6장) 등으로 구성되어 있습니다.

- (프라이버시 전자통신 규정, PECR) 동 법은 2003년에 도입되었으며 DPA 등 다른 개인정보보호 법률에서 상세히 다루지 못하고 있는 전자통신 분야의 개인정보보호에 대해 구체적인 내용을 규정하고 있습니다. 동 규정은 전자적 수단을 통한 마케팅이나 쿠키 등 이용 정보를 추적하는 경우, 공공 전자통신 서비스의 보안 영역이나 통신 네트워크나 서비스를 이용하는 이용자의 프라이버시에 대해 규율합니다.

(개인정보 국외 이전) 영국은 2022년 11월 23일 우리나라에 대한 적정성 결정을 위한 입법 절차를 완료하였습니다. 이는 영국이 EU를 탈퇴한 이후 다른 나라에 대해 적용하는 첫 번째 적정성 결정입니다. 영국의 우리나라에 대한 적정성 결정은 영국 의회에서 특별한 의견이 없을 경우 2022년 12월 19일에 최종 채택 발효될 예정입니다.

영국의 적정성 결정이 예정대로 최종 채택·발효되면 우리나라의 영국 내 기업들은 개인정보의 국외 이전 규정과 관련해서는 영국 국민의 개인정보를 별다른 절차나 인증 없이 국내로 이전할 수 있게 됩니다.



5.해외 GDPR 관련 가이드 발간 현황

국가명	발행기관	가이드제목	발행일	URL
Japan	日本貿易振興機構 (JETRO ジェトロ) ブリュッセル事務所 海外調査部 欧州ロシア CIS 課	「EU 一般データ保護規則 (GDPR)」 に關わる実務ハンドブック (入門編)	2016.11.	https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html
		「EU 一般データ保護規則 (GDPR)」 に關わる実務ハンドブック (実践編)	2017.08.	https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html
France	CNIL(Commission Nationale de l'Informatique et des Libertés)	General Data Protection Regulation GUIDE FOR PROCESSORS SEPTEMBER 2017 EDITION	2017.09.	https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf
		Le règlement général sur la protection des données - RGPD	2018.05.23.	https://www.cnil.fr/fr/reglement-europeen-protection-donnees
		GDPR에 따른 개인정보 영향분석 가이드라인	2018.11.06	https://www.cnil.fr/sites/default/files/atoms/files/journal_officiel_de_la_republique_francaise_-_ndeg_326_du_6_novembre_2018.pdf
		Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur(notamment aux cookies et autres traceurs)(rectificatif)	2019.07.19.	https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337

France	CNIL & CADA (la Commission d'accès aux documents administratifs)	쿠키 및 기타 추적에 대한 지침	2020.09.17	https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf
		GUIDE PRATIQUE DE LA PUBLICATION EN LIGNE ET DE LA RÉUTILISATION DES DONNÉES PUBLIQUES	2019.12.17.	https://www.cnil.fr/fr/open-data-la-cnil-et-la-cada-publient-un-guide-pratique-de-la-publication-en-ligne-et-de-la
Ireland	DPC (Data Protection Commission)	Data Sharing in the Public Sector	2019. 04.	https://www.dataprotection.ie/en/guidance-landing/data-sharing-public-sector
		Guidance for Organisations Engaging Cloud Service Providers	2019. 10.	https://www.dataprotection.ie/en/guidance-landing/guidance-organisations-engaging-cloud-service-providers
	HRB (Health Research Board)	GDPR guidance for health researchers	2018.10	https://www.hrb.ie/funding/gdpr-guidance-for-researchers/
Australia	OAIC (Office of Australian Information Commissioner)	Guide to health privacy	2019. 09.	https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/
U.S	CTA (Consumer Technology Association)	GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH AND WELLNESS INFORMATION	2019. 09.	https://cdn.cta.tech/cta/media/media/advocacy/pdfs/cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf
United Kingdom	ICO (Information Commissioner's Office)	Guide to the General Data Protection Regulation(GDPR)	2019. 05. 22.	https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
Germany	Bundesministerium der Justiz und für Verbraucherschutz, Bundesamt für Justiz	Federal Data Protection Act(BDSG)	2017. 06. 30.	https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf

Nether lands	AP(Autoriteit Persoonsgegevens)	Handreiking cross-sectorale gegevensdeling tussen private partijen (Guidelines for cross-sectoral blacklists)	2021.07.15	AP(Autoriteit Persoonsgegevens)
Spain	AEPD (Agencia Española de Protección de Datos)	Guidelines for Data Protection by Default	2020.10	https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto-en.pdf
		Blockchain (II): Basic concepts	2020.11.20	https://www.aepd.es/en/prensa-y-comunicacion/blog/blockchain-ii-basic-concepts
		Blockchain (III): Smart Contracts and personal data	2022.03.14	https://www.aepd.es/en/prensa-y-comunicacion/blog/blockchain-iii-smart-contracts-and-personal-data
European Union	EDPB(European Data Protection Board)	Guidelines 06/2022 on the practical implementation of amicable settlements	2022.05.12	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062022-practical-implementation-amicable_en
		Guidelines 02/2022 on the application of Article 60 GDPR	2022.03.14	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022022-application-article-60-gdpr_en
		Guidelines 04/2021 on Codes of Conduct as tools for transfers	2022.02.22	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_en
		Guidelines 01/2021 on Examples regarding Personal Data Breach Notification	2022.01.03	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

European Union	EDPB(European Data Protection Board)	Guidelines 10/2020 on restrictions under Article 23 GDPR	2021.10.13	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en
		Guidelines 07/2020 on the concepts of controller and processor in the GDPR	2021.07.07	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
		Guidelines 8/2020 on the targeting of social media users	2021.04.13	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en
		Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679	2021.03.09	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092020-relevant-and-reasoned-objection-under_en
		Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications	2021.03.09	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en
		Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies	2020.12.15	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en
		Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR	2020.12.15	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en
		Guidelines 4/2019 on Article 25 Data Protection by Design and by Default	2020.10.20	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

European Union	EDPB(European Data Protection Board)	Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)	2020.07.07	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en
		Guidelines 05/2020 on consent under Regulation 2016/679	2020.05.04	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
		Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak	2020.04.21	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en
		Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak	2020.04.21	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en
		Guidelines 3/2019 on processing of personal data through video devices	2020.01.30	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
		Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation	2019.11.12	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
		Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects	2019.10.16	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en
		Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0	2019. 06. 04.	https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it

European Union	EDPB(European Data Protection Board)	Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation(2016/679) Version 3.0	2019. 06. 04	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en
		Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation(2016/679) - Annex 1 Version for public consultation	2018. 12. 04.	https://edpb.europa.eu/our-work-tools/public-consultations/2018/edpb-guidelines-42018-accreditation-certification-bodies_en
		Guidelines 3/2018 on the territorial scope of the GDPR(Article 3) - Version for public consultation	2018. 11. 16.	https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en
		Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679	2018. 05. 25.	https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en
		Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation Version 3.0	2019. 06. 04.	https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en
		Endorsement 1/2018 EDPB	2018. 01.	https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en.pdf
	ARTICLE 29 DATA PROTECTION WORKING PARTY	Guidelines on Article 49 of Regulation 2016/679 (WP262)	2018. 02. 06.	https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en

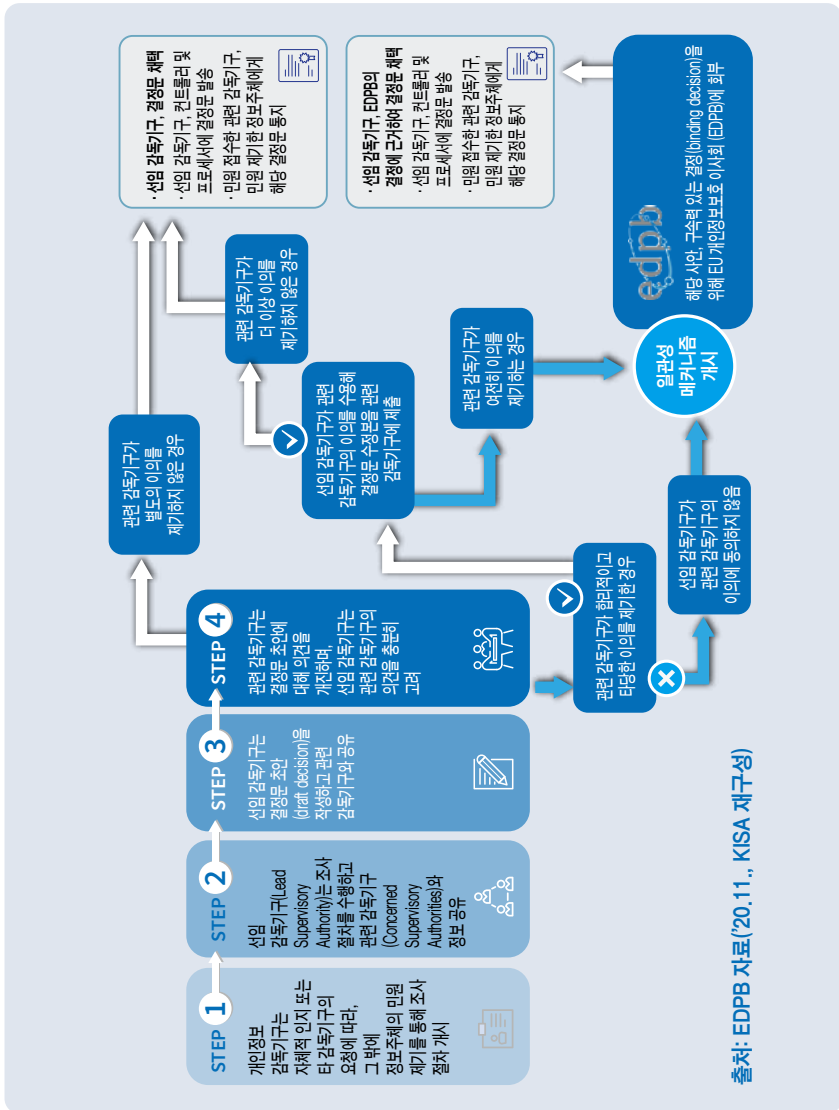
European Union	ARTICLE 29 DATA PROTECTION WORKING PARTY	Draft Guidelines on the accreditation of certification bodies under Regulation(EU) 2016/679 (WP261)	2018. 12. 06.	https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877
		Guidelines on transparency under Regulation 2016/679 (WP260rev.01)	2018. 04. 11.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
		Guidelines on consent under Regulation 2016/679 (WP259rev.01)	2018. 04. 10.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
		Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251)	2018. 02. 06.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
		Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)	2018. 02. 06.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
		Guidelines on the Right to data portability (WP242rev.01)	2017. 04. 05.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
		Guidelines on Data Protection Impact Assessment(DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP248rev.01)	2017. 10. 04.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
		Guidelines on Data Protection Officers(‘DPOs’) (WP243rev.01)	2017. 04. 05.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
		Guidelines for identifying a controller or processor’s lead supervisory authority (WP244rev.01)	2017. 04. 05.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

European Union	ARTICLE 29 DATA PROTECTION WORKING PARTY	POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR	2018. 04. 19.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045
		Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR	2018. 04. 11.	https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29GruppeEDSA/SonstigePapiere/WP263_EN.html
		Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data	2018. 04. 11.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623850
		Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data	2018. 04. 11.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848
		Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules	2018. 02. 06.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109
		Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules	2018. 02. 06.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110
		Working document on Adequacy Referential(WP254rev.01)	2018. 02. 06.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
		Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253)	2017. 10. 03.	https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

European Union	Official Journal of the European Union	REGULATION(EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(General Data Protection Regulation)	2016. 04. 05.	https://eur-lex.europa.eu/eli/reg/2016/679/oj
----------------	--	--	---------------	---



원스톱 메커니즘



찾아보기

A

adequacy decision 25, 208, 209, 213, 214, 270

B

BCR 216, 222, 223, 224, 225, 226, 270

Brexit 280, 281

C

certification 25, 26, 167, 192, 195, 210, 270, 287, 288

code of conduct 25, 210, 270

D

Data protection by design and by default

18, 24, 27, 31, 167, 168, 172, 170, 173, 174, 178, 224, 255

Data Protection Officer 24, 27, 167, 184, 189, 191, 198, 269, 288

DPO 18, 24, 27, 35, 71, 73, 127, 167, 168, 171, 179, 180, 183, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 198, 199, 198, 200, 224, 234, 236, 254, 269, 273, 274, 279, 291

E

EDPB 49, 52, 56, 62, 81, 87, 89, 177, 186, 191, 195, 209, 214, 232, 246, 284, 285, 286, 287

ePrivacy 87

L

lead supervisory authority 32, 33, 288, 291

O

One stop shop 23

R

Right to be forgotten 123, 124, 142, 286

Right to data portability 123, 124, 149, 288

S

SCC 214, 216, 217, 221, 260, 274

supervisory authority 26, 32, 33, 173, 245, 264, 288, 291

ㄱ

가명정보 52, 267

가명처리 22, 28, 31, 36, 37, 50, 52, 68, 69, 79, 172, 173, 194, 272

감독기구 19, 23, 25, 26, 32, 33, 35, 43, 116, 128, 129, 137, 140, 151, 173, 174, 177, 179, 180, 181, 183, 184, 186, 194, 195, 198, 199, 200, 209, 210, 216, 219, 220, 222, 223, 225, 226, 230, 232, 233, 234, 235, 236, 237, 239, 240, 241, 242, 245, 246, 250, 251, 253, 255, 256, 257, 260, 261, 269, 270, 271, 278, 291

개인정보 영향평가 23, 24, 73, 102, 162, 167, 168, 169, 171, 175, 176, 177, 178, 179, 180, 181, 182, 183, 189, 190, 200, 201, 270

개인정보 이동권 18, 24, 89, 92, 97, 123, 124, 149, 150, 151, 152, 269

거부권 18

고지의무

공적 업무 수행 74, 75, 94, 95, 96, 97, 153, 154

공정성 22, 46, 47, 48, 50, 52, 60, 127, 159, 161, 163

과징금 26, 46, 52, 71, 119, 134, 135, 168, 173, 174, 180, 186, 215, 237, 241, 244, 249, 250, 251, 253, 254, 255, 256, 257, 258, 271

과학적 연구 80, 97, 155

구속력 있는 기업규칙 211, 217

구제 수단 25, 245, 246,

기밀성 22, 46, 69, 70, 230, 234, 238, 239, 240,

C

동의의 유효 요건 82, 104, 105

동의의 철회 107, 110

Q

명시적 동의 22, 25, 38, 94, 104, 109, 110, 118, 159, 210, 218, 219, 270, 274

목적 제한 22, 46, 49, 50, 52, 163, 224, 251

무결성 22, 46, 69, 70, 230, 238

민감정보 21, 25, 28, 30, 34, 38, 45, 47, 49, 52, 54, 75, 79, 83, 89, 92, 93, 94, 95, 104, 111, 117, 118, 117, 119, 120, 160, 170, 177, 180, 183, 184, 185, 186, 187, 202, 203, 221, 224, 236, 249, 255, 269, 270, 274, 275

H

반대권 18, 24, 77, 85, 89, 92, 97, 102, 103, 123, 124, 153, 154, 155, 164

벌칙 19, 244, 252, 258

범죄정보 45, 47, 49, 54, 75, 79, 89, 104, 117, 118, 119, 120, 177, 184, 185, 203

법적 의무 22, 74, 75, 76, 77, 85, 86, 89, 90, 91, 92, 143, 144, 177, 256, 268, 277, 278

보상 186, 224

人

삭제권 18, 24, 54, 56, 57, 62, 63, 64, 69, 92, 97, 116, 123, 124, 142, 143, 144, 145, 151, 155, 164, 268

손해배상 의무 247, 248

손해배상청구권 244, 247, 248

O

아동 개인정보 22, 45, 112, 115

안전조치 52, 69, 70, 73, 102, 106, 137, 160, 214

양립가능성 37, 79

역사적 연구 37, 51, 68, 119, 144, 153, 155

역외미전 218, 220, 274, 276

원스톱숍 메커니즘 23, 260, 291

인증 25, 26, 71, 73, 151, 152, 167, 168, 183, 192, 193, 195, 196, 197, 209, 210, 217, 220, 223, 225, 250, 255, 256, 257, 270, 271, 281

잊힐 권리 123, 124, 142, 143, 144, 145, 268

ㅈ

자동화된 의사결정 24, 83, 111, 116, 123, 124, 137, 156, 157, 158, 160, 161, 163, 164, 171, 202, 203

자유로운 동의 105

적법성 47, 222, 225

적법처리기준

적법한 이익 23, 74, 75, 77, 78, 79, 85, 86, 94, 97, 98, 99, 100, 101, 102, 103, 127, 134, 135, 153, 154, 160, 171, 178, 194, 219

적절한 안전조치 137

적정성 결정 25, 107, 127, 208, 209, 210, 211, 213, 214, 215, 217, 218, 219, 220, 274, 281

접근권 24, 28, 49, 64, 67, 123, 124, 136, 137, 138, 164, 257

정보주체 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 36, 38, 39, 42, 43, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 58, 59, 60, 62, 63, 64, 65, 67, 68, 70, 71, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 90, 92, 94, 95, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 114, 116, 118, 119, 120, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 168, 170, 171, 173, 177, 178, 179, 180, 183, 184, 185, 188, 190, 194, 197, 199, 201, 202, 203, 204, 205, 209, 210, 215, 218,

219, 220, 221, 223, 224, 230, 232, 233, 234,
235, 236, 237, 238, 239, 240, 241, 242, 245,
246, 247, 249, 253, 254, 257, 267, 268, 269,
270, 271, 272, 274, 275, 276, 279, 291

정정권 20, 24, 54, 55, 56, 62, 123, 124, 139, 140,
141, 164

정확성 22, 46, 53, 57, 58, 59, 61, 62, 63, 139,
140, 146, 163

주 감독기구 23, 32, 33, 239

중대한 이익 74, 75, 77, 93, 94, 118, 219

ㄸ

책임 18, 19, 33, 35, 70, 71, 72, 73, 78, 81, 98,
114, 129, 133, 143, 152, 154, 161, 166, 168, 171,
176, 180, 184, 191, 192, 194, 224, 231, 244, 246,
247, 248, 254, 257, 267, 268, 271, 279

책임성 18, 22, 24, 46, 70, 71, 72, 78, 80, 97, 101,
124, 134, 162, 166, 168, 169, 171, 173, 175, 177,
179, 181, 183, 185, 187, 191, 193, 195, 197, 199,
201, 203, 205, 235, 275, 279

처리제한권

최소한의 개인정보 53, 98

친권자 동의 112, 113, 114

침해 사고 229, 230, 231, 233, 235, 251

침해 통지 24, 32, 73, 194, 228, 232, 233, 234,
237, 238

ㄷ

컨트롤러 19, 22, 23, 24, 25, 27, 29, 30, 32, 33,
34, 35, 36, 39, 40, 41, 43, 46, 50, 51, 53, 54, 57,
60, 64, 65, 66, 67, 70, 71, 72, 73, 74, 75, 79, 80,
81, 82, 83, 84, 85, 86, 87, 89, 90, 92, 96, 97,
98, 99, 100, 101, 102, 103, 105, 106, 107, 108,
109, 110, 113, 114, 116, 117, 118, 119, 120, 124, 126,
127, 129, 130, 131, 132, 133, 134, 136, 137, 138,
139, 140, 141, 142, 143, 144, 146, 147, 149, 150,

151, 152, 153, 154, 155, 158, 159, 160, 161, 162,
168, 169, 170, 171, 173, 175, 177, 178, 179, 180
184, 185, 188, 189, 190, 191, 192, 193, 194, 195,
197, 198, 199, 200, 204, 209, 213, 215, 216, 217,
218, 219, 220, 221, 222, 224, 229, 231, 232,
234, 235, 236, 237, 239, 240, 241, 242, 246,
247, 248, 249, 250, 253, 254, 255, 256, 257,
260, 268, 269, 271, 272, 273, 274, 275, 291

ㅁ

투명성 22, 26, 46, 47, 48, 49, 50, 51, 52, 60, 78,
80, 97, 102, 106, 124, 126, 129, 131, 132, 133,
135, 158, 161, 163, 179, 193, 195, 197, 251

ㅂ

프로세서 19, 23, 24, 27, 30, 32, 33, 34, 35, 36,
39, 40, 41, 70, 73, 118, 169, 170, 171, 173, 179,
183, 184, 185, 189, 190, 191, 192, 193, 195, 197,
198, 199, 200, 209, 215, 216, 217, 218, 221, 222,
224, 235, 238, 246, 247, 248, 249, 250, 254,
255, 256, 257, 268, 269, 271, 272, 273, 274,
275, 291

프로파일링 24, 30, 77, 83, 85, 86, 87, 107, 111,
123, 124, 128, 137, 150, 153, 154, 156, 157, 158,
159, 160, 161, 162, 163, 164, 171, 177, 251, 275

ㅇ

행동규약 25, 71, 73, 116, 167, 168, 178, 192, 193,
194, 195, 197, 209, 210, 217, 220, 250, 255, 256,
257, 270

집필진·자문·감수

연구책임기관	<ul style="list-style-type: none">개인정보보호위원회한국인터넷진흥원 개인정보협력팀	
집필책임	최경진 교수	(가천대학교)
집필진	이창범 교수	(동국대학교)
	강태욱 변호사	(법무법인 태평양)
	윤수영 이사	(PMK)
	고환경 변호사	(법무법인 광장)
	채상미 교수	(이화여자대학교)
감수·자문	이인호 교수	(중앙대학교)
	김일환 교수	(성균관대학교)
	박광배 변호사	(법무법인 광장)
	김진환 변호사	(김앤장법률사무소)
	정지연 사무총장	(한국소비자연맹)
개정·증보	넥스텔리전스㈜	

우리 기업을 위한
2022 EU일반개인정보보호법(GDPR) 가이드북

발행일	2022년 11월
발행처	한국인터넷진흥원 (58324) 전라남도 나주시 진흥길 9 Tel. 1433-25
디자인·제작	이영진, 이건하
교정 및 윤문	정우진, 서겸손, 신세연, 김윤정

문의 E-mail : gdpr@kisa.or.kr

- 이 가이드북은 개인정보보호위원회의 출연사업금으로 수행한 개인정보보호 협력체계 구축 사업의 결과입니다.
- 이 가이드북의 내용을 발표할 때에는 반드시 한국인터넷진흥원 ‘개인정보보호 협력체계 구축 사업’ 결과임을 밝혀야 합니다.
- 가이드북에 포함되어 있는 내용은 향후 EU 집행위원회 GDPR 전체의 내용을 포함하지 않을 수 있으며, 유권 해석 및 판례에 따라 그 내용이 달라 질 수 있습니다.
- 이 가이드북의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.