Global Strategy Report 18-002

대한민국의 꿈을 수출합니다 kotra

2018

Global Strategy Report

EU의 일반개인정보보호법(GDPR) 발효와 대응과제

kotra
Korea Trade-Investment Promotion Agency

CONTENTS

목 차

요 약

□ **EU는 2018년 5월 25일부터** 개인정보 처리와 이동에 관한 **"일반개인정보보호법(General Data Protection Regulation: 이하 GDPR)" 시행**

○ GDPR은 EU 회원국 모두에게 동일하게 적용되는 개인정보보호 일반법으로 우리나라의 개인정보보호법과 유사한 성격

○ **GDPR은 4차산업혁명 시대의 새로운 규제 패러다임을 제시, 한국을 비롯한 각국 개인정보 보호법제의 벤치마크가 될 전망**

□ **GDPR은 기업 규제환경의 큰 변화를 초래하여, EU 역내 투자기업은 물론, EU 거주민을 대상으로 하는 다양한 기업 활동에 영향**

○ **(넓은 지리적 적용범위)** EU 역내에서 거점(establishment)을 운영하면서 그 활동이 개인정보의 처리를 포함하는 경우는 물론, 역외에 위치하면서 EU 거주 정보주체에게 재화·서비스 제공하는 경우에도 적용*

* 예: 유럽 대상 전자상거래 수출 기업, 시청각콘텐츠 공급 기업, 소비재와 IoT를 결합한 B2C 비즈니스를 추진하는 제조기업 등

– 또한 역외로 이전된 정보를 제3국으로 다시 이전하여 처리할 경우에도 적용

○ **(개인정보 범위의 확대) IP 주소, 쿠키, RFID(radio frequency identification tags), 위치정보 등도** 개인정보로 간주되며, **민감 개인정보**를 규정하고 **유전정보와 바이오정보 등**을 포함

○ **(개인정보 국외이전 메커니즘) 적정성 평가* 또는 구속력 있는 기업규칙(Binding Corporate Rules), 표준계약서(Standard Contractual Clauses)*, 인증(Certificate) 등**을 통한 국외 이전 가능

* 한국은 EU로부터 적정한 개인정보 보호조치를 운영하는 것으로 인정받기 위해 적정성 평가(adequacy decision)를 진행 중

* BCR은 기업 내부 이전시 활용, 표준계약조항은 EU 집행위가 제시한 규정에 준함.

○ **정보주체의 권리와 정보 프로세서의 의무 강화, 기업의 DPO(Data Protection Officer)* 임명 의무 등 책임성 강화**

* DPO는 기업 내의 GDPR 등 정보보호 법규 이행상황을 모니터링하는 등의 업무 수행

□ **GDPR은 통합된 EU 디지털시장을 창출하는 데 기여할 전망이나, 단기적으로 장벽 요인으로 작용하여 기업 활동에 부정적 영향을 줄 가능성 내포**

○ **역내 규제 조화를 통해 시장을 확대하고, 혁신을 촉진**할 것으로 기대

○ 그러나 **기업들이 당분간 상당한 적응비용을 부담하고, 불확실성에 직면**

– 개인정보 활용 제약에 따른 역내 투자기업의 비즈니스 혁신 둔화 가능성

– EU 역내기업이 법 적용의 불확실성을 우려하여 서비스 조달처를 역내로 전환하거나 데이터 분석 업무를 직접 수행할 경우, 역외기업의 수출·투자에 부정적 영향

○ **우리나라는 對EU 무역투자 특성상 GDPR 대응에 노력을 기울일 필요성이 높음.**

– 우리 기업과 스타트업의 최근 對EU 진출은 데이터 혁신과 직간접적으로 연계된 전자·전기, 소비재, 통신업, 정보서비스업 등이 중심

□ **GDPR을 단순히 규제요인으로 인식할 것이 아니라, 개인정보보호 규제 컴플라이언스 수준을 높이는 기회로 활용할 필요**

○ **개인정보 보호역량 강화를 통해 기업 경쟁력 강화, 신뢰도 향상***

* 영국 사례: 개인정보 제공이 필요한 거래에서 기업에 대한 신뢰도가 경제적 동기(저렴한 상품 구매 등)보다 더 중요하게 작용

○ **국내외 인증제도를 활용하여 개인정보 보호 역량 강화**

– ISO 27001 획득은 글로벌 비즈니스의 필수조건, GDPR 이행에도 기여

○ **선진적인 개인정보 보호체제 도입**

– 개인정보보호 영향평가 도입*, 개인정보책임자(DPO)** 확보·역량 강화 등

* 한국은 공공부문만 의무로 규정하나, GDPR의 경우와 같이 민간으로 확대되는 추세

** DPO는 개인정보 관련 기술·법률적 지식을 두루 갖춘 인력

○ **산업 생태계 차원의 개인정보 체제 구축**

– GVC의 성숙과 더불어 해외 협력업체의 개인정보 보호역량도 중요해지고 있는바, 보안조치에 대한 협력 파트너간 상호계약 등이 요구됨.

Ⅰ 서론

1 연구 배경

가. GDPR 도입

□ **EU는 2018년 5월 25일부터 "일반개인정보보호법**(General Data Protection Regulation: 이하 GDPR)"[1] **시행**

○ EU는 2016년 5월 개인정보의 처리와 이동에 관한 자연인(정보주체) 보호를 목적으로 하는 GDPR 발표

○ 개별 회원국은 국내법 개정을 거쳐 2018년 5월 25일부터 적용

– GDPR은 EU 회원국 모두에게 동일하게 적용되는 개인정보보호 일반법으로서, 우리나라의 개인정보보호법과 유사한 지위

□ GDPR 도입 목적은 ① 4차산업혁명 시대에 대응한 **개인정보 보호체제 확립**, ② **역내 디지털 혁신을 촉진하기 위한 통일된 규제여건 조성**

○ 온라인 상의 개인정보 유출 우려에 대응하여 개인(정보주체)에게 개인정보에 대한 더 많은 통제권 부여

– EU 거주자의 개인정보가 국외로 이전될 시 적절하게 보호받는지도 EU의 주요 관심사

○ 회원국들의 개인정보보호법을 통일함으로써 역내 규제 환경 개선을 개선하여 디지털 혁신을 촉진

– 개인정보보호체제의 호환성을 높이는 것은 EU 역내 시장 확대의 중요 조건

– EU는 GDPR을 도입하여 인터넷 서비스 플랫폼, 사물인터넷, 클라우드컴퓨팅,

1) 공식 명칭: 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)

빅데이터, 보안산업 등에 걸쳐 역내 데이터 혁신을 가속화한다는 복안

나. 개인정보가 기업활동에 갖는 의미

□ 개인정보는 4차산업혁명의 핵심 자원·연료

○ 디지털화를 통한 혁신은 대규모의 데이터 수집·처리·이동을 수반하며, 다양한 종류의 데이터 가운데서도 개인정보는 가장 주요한 부가가치 창출원

– 세밀한 개인정보 수집, 인공지능과 빅데이터 분석의 적용을 통해 **개인정보는 맞춤형 제품·서비스 개발의 기초자원**

○ 사물인터넷 사례: 냉장고에 부착된 센서를 통해 사용자의 행태정보 수집 → 정보 축적 → 정보 분석 → 냉장고가 쇼핑할 식료품을 미리 제안(피드백)

– 개인별 행태정보를 축적하여 적절히 분석하면 더 나은(개인화된 맞춤형) 서비스 제공 가능

○ 파편화된 정보를 결합하여 특정 개인을 식별할 수 있는 분석기술이 발달하면서 '잠재적인 개인정보' 확대

– 이름·주소·이메일주소·계좌변호 등 통상적인 개인정보 이외에, IP 주소, 단말의 유심번호 등도 他정보와 결합되어 개인 식별에 활용됨.

○ 글로벌기업들이 데이터 혁신을 주도하는 가운데, 후발 기업들 역시 데이터(개인정보)를 활용한 사업모델 개발을 통해 新시장 모색

– 데이터를 활용한 혁신은 제조업, 의료보건, 전력 등 다양한 산업에서 가능

♣ GM의 온스타 서비스(커넥티드카 서비스)를 통해 수집되는 정보 ♣

- **사물인터넷 단말(센서)에서 수집되는 개인정보**: 위치정보, 이동·운전습관 정보(주행일자, 이동경로, 거리, 운행시간, 평균속도 등), 취향·생활습관 정보(통화이력, 쇼핑, 음악 취향정보, 목적지 빈도 등), 차량상태 정보
- **사물인터넷 네트워크 단에서 수집되는 사용자 식별 가능 네트워크 정보**: 모바일 식별번호(MEID: Mobile Equipment Identifier), 국제 이동가입자 식별번호(IMSI: Int'l Mobile Subscriber Identity), 블루투스의 스펙 ID(Specification ID) 등
- **서비스 플랫폼에서 수집·관리되는 개인정보**: 개인신상정보(성명, 주소, 전화번호, 이메일 등), 서비스 관련 정보(차량식별번호, 서비스 사용 로그 등), 금융결제정보(신용카드 정보 등)

자료: 김범수·이애리(2017)

□ 개인정보의 활용이 중요한 시점이지만, 온라인 상의 개인정보 유출·오남용 가능성도 높아져, **EU를 포함한 많은 국가들이 개인정보 보호체제를 개선 중**

○ 우리나라는 개인정보의 활용을 촉진하면서 동시에 적정한 보호체제를 도입하기 위한 목적으로 개인정보보호법을 개정 중

□ **기업 활동 시 개인정보의 국경간 이전이 확산되는 추세**

○ 기업의 글로벌 활동 시 국외 개인정보의 수집과 분석이 일반화

– 글로벌 기업 뿐만 아니라, 각국에서 이들과 협력하는 기업, 해외진출 기업 등도 국외 개인정보를 이전받아 처리하는 경우가 증가

○ 최근 국제통상협상(WTO 및 TPP 등 FTA)에서는 그간 경제·통상 영역에서 다루어지지 않았던 개인정보 등 데이터의 국경간 이동이 쟁점으로 대두[2)]

2) 자세한 내용은 김정곤 외(2015) 참고.

2 연구 필요성과 내용

□ GDPR은 **EU 역내 투자기업은 물론, EU 거주민 개인정보를 취급하는 모든 기업 활동에 영향을 줄 것으로 전망**

○ GDPR은 EU 역내에서 거점(establishment)을 운영하면서 그 활동이 개인정보의 처리를 포함하는 경우는 물론, 역외에 위치하면서 EU 거주 정보주체에게 재화와 서비스를 제공하는 경우에도 적용 가능*

* 예: 유럽시장을 대상으로 하는 전자상거래 수출 기업, 시청각콘텐츠 공급 기업 등

– 또한 역외로 이전한 정보를 제3국으로 다시 이전하여 처리할 경우에도 적용

– 유럽시장을 대상으로 개별 소비자와의 접점을 확대하는 비즈니스를 추진한다면 GDPR 적용 가능성에 대한 검토가 필요*

* 예: 소비재와 IoT를 결합시키는 등의 B2C 비즈니스를 염두에 두는 제조기업

○ GDPR은 EU 차원의 개인정보 보호법 조화로서 큰 의의를 가지고 있지만, 까다로운 규정을 다수 포함

– 개인정보의 수집·해외이전 시 사용자 동의 조건 강화, 잊힐 권리(정보 삭제권) 등 소비자 권리 확대, 위반시 높은 과징금 부과 등

□ EU는 4차 산업혁명 시대 주요 협력대상국이 될 가능성이 높은바, **중소·중견기업, 스타트업의 GDPR에 대한 이해와 대응이 중요**

○ 유럽 국가들은 미국이 주도하는 디지털화 시대에 주도권을 회복하고, 새로운 성장 동력을 창출하기 위한 정책 노력 경주

– EU 국가들은 최근 산업 디지털화 전략을 본격화하고 있으며, 스타트업 투자가 급격히 증가하는 등 혁신기업에 대한 우호적인 환경 조성[3]

○ GDPR은 **개인정보 보호법제의 주요한 벤치마크로 자리매김 중**

– EU와 법제가 상이한 미국은 Privacy Shield 협정을[4] 통해 자국 기업이 EU

3) 보다 자세한 내용은 김정곤(2017) 참고.
4) EU는 적정성 평가(adequacy decision)를 거쳐 적정한 개인정보 보호수준을 갖춘 국가를 White List로 지정한다.

가 요구하는 수준의 개인정보 보호를 이행토록 함.

- 한국, 일본은 EU의 적정성 평가(adequacy decision)를 진행 중으로서, EU의 요구수준에 부합하는 개인정보 보호법제를 마련 중

□ **(보고서 내용) GDPR의 핵심적인 내용과 기업에 대한 영향 가능성을 분석하고, 우리 기업의 대응과제를 제시**

○ 첫째, 우리기업의 EU 진출 현황을 통해 GDPR의 영향가능성 점검

○ 둘째, GDPR의 주요 내용 분석과 유럽 주요국과 한국의 대응현황

○ 셋째, GDPR의 평가와 전망, 개인정보 패러다임 변화에 따른 우리 기업과 정부의 대응과제

이에 포함되지 않은 미국은 EU와의 정부간 협정인 Privacy Shield를 통해 자국기업이 EU 시민의 개인정보를 처리할 수 있도록 한다. Privacy Shield에 참여하는 미국 기업은 해당 요구 조건을 준수하는 한편, 매년 상무부에 이를 입증해야 한다. Privacy Shield를 통해 미국 정부는 자국기업의 EU 시민 개인정보 보호 이행 여부를 책임진다.

II 한국기업의 EU 진출 현황

1 수출

□ **우리나라의 對EU 수출은 2017년 EU의 경기 회복과 더불어 전년 대비 15.9% 증가한 540.4억 달러를 기록, 전체 수출의 약 9.4%를 차지***

* EU는 한국의 제3위 무역파트너. 1위는 중국(1421.2억달러, 24.8%), 2위는 미국(686.1억달러, 11.9%)

○ 2017년 對EU 수입 역시 전년 대비 10.4% 증가한 572.8억 달러

○ 무역수지 적자폭은 2014년 이후 지속 감소, 2017년 32.4억 달러

그림 II-1. 한국의 對EU 무역 추이(2013~17, 억 달러, %)

주: 무역규모 및 무역수지는 좌축, 무역 증감율은 우축.
자료: 한국무역협회 K-Stat.

□ 데이터 혁신과 직간접적으로 연계된 **전자·전기, 기계류, 소비재·식품류의 對EU 수출 호조**

○ 전자·전기제품 중에서는 TV카메라 및 수상기, 보조기억장치, 계측기, 의

료용전자기기, 센서 등의 수출이 호조, 기계류 가운데는 승용차와 의료용 기기 등의 수출이 최근 증가세

○ 전자상거래와 연관성이 높은 소비재 중에서는 면류, 음료 등 농수산식품, 위생용품을 비롯한 생활용품, 그리고 화장품과 의약품 수출이 증가세

표 Ⅱ-1. 최근 2년 연속 주요 對EU 수출 증가 품목*

품목군	품목(MTI 4단위)
전자·전기	TV카메라 및 수상기, 보조기억장치, 계측기, 의료용전자기기, 센서, 에어컨, 기타 가정용전자제품 등 34개
기계	승용차, 의료용기기 등 22개
소비재**	- 면류, 음료 등 농수산식품군 32개 - 위생용품 등 생활용품군 9개 - 의약품, 화장품 등 화학제품군 2개 등

* : 2016 및 2017년간 전년대비 수출이 연속해서 증가한 품목군을 대상으로 산출

** : 전자·전기제품에 속하는 소비재는 제외한 것임.

자료: 한국무역협회 K-Stat.

□ EU는 진입장벽이 높고 전통적으로 역내 무역의존도가 높지만, **최근 중견·중소기업이 對EU 수출에서 차지하는 비중이 증가하는 추세**

○ 對EU 수출에서 중소기업과 중견기업이 차지하는 비중은 2013년 14.9%, 15.3%에서 2016년 16.8%, 18.2%로 증가

– 일반적으로 수출초보기업이 EU시장에 진출하는 것은 어렵지만, 수출경험을 쌓은 경쟁력 있는 기업은 꾸준히 EU 시장 진출을 모색*

* 수출규모 500만 달러 이상의 기업(대기업 포함)이 對EU 수출의 약 91%를 차지(코트라. 2018)

표 Ⅱ-2. 기업규모별 對EU 수출 비중(%)

연도	중소기업	중견기업	대기업	기타
2013	14.9	15.3	69.9	0.2
2014	16.4	15.3	68.1	0.2
2015	15.5	18.5	65.9	0.1
2016	16.8	18.2	64.8	0.2

자료: 통계청. 대륙별·국가별 기업규모별 수출 통계.

□ **최근 對EU 지식재산권사용료, 통신·컴퓨터·정보서비스, 기타서비스 분야 수출이 증가하는 양상**을 보이는 것이 특징적

○ 지재권사용료는 지속적인 적자를 기록하고 있지만* 수출 규모가 늘고 있으며, 통신·컴퓨터·정보서비스 수지는 2016년 4억 1,620만 달러 흑자 기록

* 우리나라는 EU에 대해 연간 약 98억 달러(2013~16 평균)의 서비스 수지 적자를 기록. 주요인은 여행수지, 기타사업서비스수지, 운송수지, 지재권사용료수지의 적자

그림 Ⅱ-2. 對EU 지재권사용료 수지

(단위: 백만 달러)

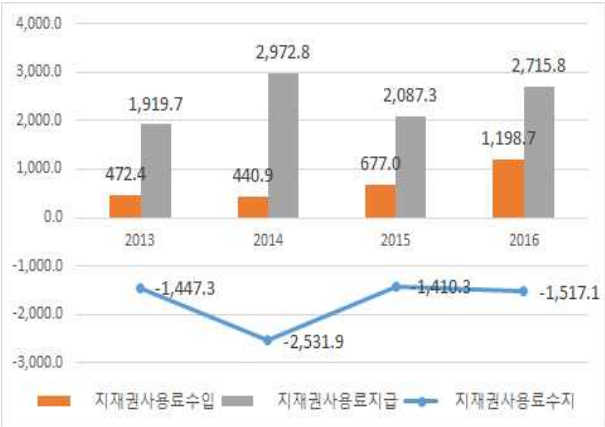


그림 Ⅱ-3. 對EU 통신·컴퓨터·정보서비스 수지

(단위: 백만 달러)

자료: 한국은행 서비스 국제수지 통계.

2 투자

□ 2013년 이후 우리 기업의 對EU 투자는 부동산·임대, 제조업 외에, **금융, 전문·과학·기술 서비스, 출판·영상·정보통신 서비스 등**에서 활발하게 진행

○ 2013~17(3분기) 對EU 투자는 약 167.6억 달러 규모로서, 700개 이상의 기업이 EU에 진출한 것으로 추산

○ 같은 기간 중 부동산·임대업 투자가 약 39억 달러로 가장 컸으며, 광업 30.2억 달러, 제조업 24.7억 달러 등을 기록

○ **GDPR과 직결될 수 있는 전문·과학·기술 서비스업에 대한 투자가 15.9억 달러, 출판·영상·정보통신 서비스업 투자가 2억 6,000만 달러로 큰 비중**

표 II-3. 한국의 주요 업종별 對EU 투자 추이(2013~17, 백만 달러)

업종(대분류)	2013	2014	2015	2016	2017 (3분기)	2013~17 업종계
부동산업 및 임대업	435.57	627.53	1094.18	1054.12	686.84	3898.25
광업	1213.54	1042.47	356.67	233.07	170.57	3016.32
금융 및 보험업	630.92	561.10	291.77	402.15	761.51	2647.46
제조업	668.90	390.55	421.00	539.97	445.97	2466.40
도・소매업	209.14	205.91	82.42	119.84	1403.18	2020.50
전문・과학・기술 서비스업	367.12	484.55	124.33	106.26	505.34	1587.60
전기・가스・증기・수도사업	89.43	65.72	3.54	0.44	263.06	422.17
출판・영상・방송통신・정보서비스업	42.01	96.11	35.82	43.30	42.06	259.30
건설업	15.41	26.70	15.06	21.77	76.07	155.01
운수업	65.21	22.71	37.03	19.24	10.18	154.38
사업시설관리・사업지원서비스업	87.65	1.62	1.27	0.67	1.69	92.90
숙박・음식점업	1.25	5.89	3.34	1.51	0.47	12.46
농림어업	0	0.54	1.08	0	7.10	8.72
예술・스포츠・여가관련서비스업	0	0.84	2.01	3.02	1.85	7.73
연도별 투자 총계	3827.00	3533.72	2470.59	2545.72	4379.87	16756.91

자료: 수출입은행 해외투자통계.

□ 전문·과학·기술 서비스업 가운데서는 **전문서비스업** 투자가 주종을 이루며, 출판·영상·정보통신 서비스업에서는 **통신업, 출판업, 정보서비스업**이 큰 비중을 차지

○ 2013~17(3분기) 기간 중 전문서비스업 투자 규모는 약 14억 달러

○ 같은 기간 중 통신업 투자규모는 9,039만 달러, 출판업은 8,537만 달러, 정보서비스업은 5,248만 달러 기록

표 Ⅱ-4. 전문·과학·기술 및 출판·영상·정보통신 서비스 對EU 투자 추이(2013~17, 백만 달러)

업종 (대분류)	업종 (중분류)	2013	2014	2015	2016	2017	합계
전문·과학·기술 서비스업	건축기술, 엔지니어링 및 기타 과학기술 서비스업	16.48	1.96	0.56	0.57	0.79	20.36
	기타 전문, 과학 및 기술 서비스업	5.53	8.83	1.01	5.88	5.65	26.89
	연구개발업	0.85	73.57	13.66	35.14	27.02	150.24
	전문서비스업	344.26	400.19	109.11	64.66	471.90	1390.11
소계		367.12	484.55	124.33	106.26	505.34	1587.60
출판·영상·방송통신·정보서비스업	방송업	0	0	0	0.93	0.21	1.14
	정보서비스업	0.01	51.94	0.01	0.52	0.00	52.48
	출판업	5.19	5.69	28.22	33.83	12.45	85.37
	컴퓨터 프로그래밍, 시스템 통합 및 관리업	0	6.74	6.01	6.27	10.9	29.91
	통신업	36.81	31.74	1.59	1.75	18.5	90.39
소계		42.01	96.11	35.82	43.30	42.06	259.30

자료: 수출입은행 해외투자통계.

3 스타트업

□ 한국 창업기업의 유럽 진출은 전문·과학·기술 서비스, 출판·영상·정보통신 서비스, 교육서비스업 등에서 활발

○ 해외 진출 창업기업 가운데 68.3%가 동북아, 29.0%가 동남 아시아에 진출하고 있으며, 북미 진출 기업은 10.3%

○ 유럽 진출 창업기업의 비중은 8.1%로 상대적으로 낮지만, **개인정보 활용 빈도가 높은 고부가 서비스업종 비중이 큼.**

표 II-5. 한국 창업기업의 주요 업종별 해외진출 지역(개, %)

업종	기업수	동북 아시아	동남 아시아	중앙 아시아	남아 시아	서남 아시아	유럽	북미	중남미	오세 아니아	아프 리카
제조업	14,720	70.5	23.6	3.8	3.9	1.4	10.2	13.4	4.3	1.9	1.9
광업	2	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
건설업	613	16.5	19.2	65.5	16.5	0.0	0.0	18.0	0.0	0.0	0.0
운수업	851	65.7	66.4	34.3	17.6	17.6	0.0	0.0	13.5	0.0	0.0
출판, 영상, 방송통신 및 정보서비스업	1,301	54.8	36.1	5.6	5.6	5.6	14.8	20.1	9.8	5.6	5.6
사업시설관리 및 사업 지원 서비스업	423	29.6	52.6	8.0	17.0	17.4	33.4	17.0	25.6	9.0	0.0
전문 과학, 기술 서비스업	1,472	61.7	25.9	1.9	8.6	4.9	40.2	26.6	3.5	8.6	13.3
보건업 및 사회복지 서비스업	180	100.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
농업, 임업, 어업	11	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
전지, 가스, 증기 및 수도사업	-	-	-	-	-	-	-	-	-	-	-
도매 및 소매업	11,686	76.0	31.4	15.8	9.9	9.9	0.0	2.6	2.4	0.0	0.0
숙박 및 음식점업	-	-	-	-	-	-	-	-	-	-	-
금융 및 보험업	60	0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
예술, 스포츠 및 여가 관련 서비스업	112	52.3	0.0	26.2	0.0	0.0	0.0	21.5	0.0	0.0	0.0
하수폐기물 처리, 원료 재생 및 환경복원업	181	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
교육서비스업	804	0.0	23.8	0.0	0.0	0.0	25.2	25.2	0.0	25.7	0.0
수리 및 기타개인서비스업	-	-	-	-	-	-	-	-	-	-	-
임대업(부동산 제외)	114	100.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

주: 설문조사 결과로서, 진출지역 복수응답.
자료: 창업진흥원(2017).

□ 유럽 스타트업 생태계는 최근 눈부신 발전을 보이면서 해외 스타트업 유치에 적극적

○ 유럽의 스타트업 투자규모는 2008년 15억 7,000만 유로에서 2016년 63억 8,000만 유로로 약 4배 증가

○ 도시별로는 런던의 스타트업 투자 규모가 127 억 유로이며, 스톡홀름 41억 유로, 베를린 39억 유로, 파리 37.4억 유로 등 주요 스타트업 생태계 구성

○ 구글, 페이스북, 아마존, 소프트뱅크, 네이버 등의 거점지로 부상

그림 Ⅱ-4. 유럽의 스타트업 투자 추이

(단위: 10억 유로)

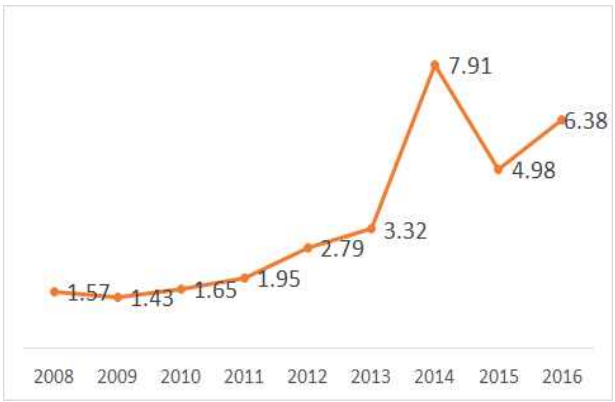
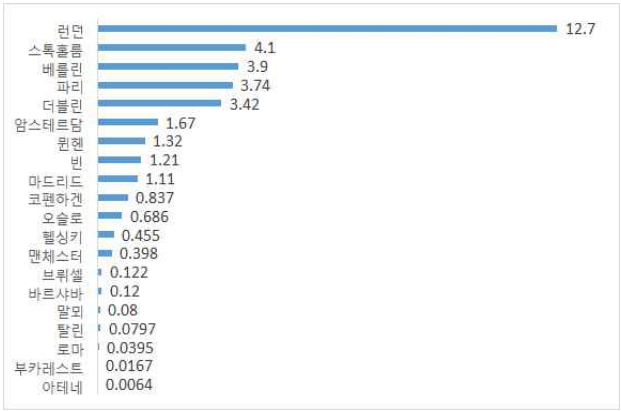


그림 Ⅱ-5. 유럽 도시별 스타트업 투자 규모

(단위: 10억 유로)



자료: Startup Hubs Europe 웹페이지.

□ 유럽 국가들은 **기업 친화적 정책, 효율적인 창업관련 법, 풍부한 자본, 외국인 친화적인 비즈니스 환경 등 강점** 보유

○ 유럽 스타트업 생태계는 글로벌 개방성이 높은바, 고객의 **20.7%가 非유럽권으로서, 他지역 평균 12.8%를 상회**(Startup Genome. 2017)

○ **(사례)** 프랑스는 저성장과 청년 실업률을 완화를 위해 2013년부터 스타트업 생태계 조성을 위한 **프렌치 테크**(La French Tech) 추진

– 프랑스 정부는 해외 스타트업 유치에 매우 적극적*

* **라 프렌치 테크 티켓(La French Tech Ticket):** 해외 스타트업의 프랑스 진출 지원 프로그램. 해외 스타트업을 선정하여 자금·정착 지원

Ⅲ GDPR의 내용과 기업의 준비과제

1 GDPR의 개요

가. 제정 배경과 목적

□ EU는 2016년 일반개인정보보호법(General Data Protection Regulation, 이하 GDPR)을 제정하여 2018년 5월 25일부터 시행[5)]

○ 이 법은 EU의 개인정보보호법제에서 일반법적 지위를 누리던 1995년 개인정보보호지침(Data Protection Directive, DPD)을 대체

– 1995년 지침이 그 목적과 원칙에 관한 한 여전히 유효하지만, 법형식이 '지침'이기 때문에 가이드라인 역할로 제한

○ 그동안 회원국별로 개인정보보호법제도가 달라 EU 전체의 법집행 측면에서 단편화와 법적 불확실성 존재

□ GDPR은 자연인의 개인정보 보호 권리를 지키고, EU 역내에서 개인정보의 자유로운 이동(제1조 제2, 3항)을 보장하는 데 목적을 둠.

○ EU의 도입 취지: ① 보다 강하고 일관성 있는 EU 차원의 개인정보보호체제를 확립함으로써 디지털경제를 발전시키고, ② 개인에게 더 많은 자기정보 결정권 부여하며, ③ 사업자에게는 법무·실무적 확실성 담보

나. 법적 성격

□ GDPR은 종래의 지침과 달리 법적 구속력을 가지며 모든 EU 회원국에 직접 적용(제99조)

○ 기존 개인정보보호지침은 GDPR 시행에 따라 폐지

5) 본장의 1, 2절은 행정안전부·한국인터넷진흥원(2017a, 2017b)을 기본 토대로 작성되었다.

□ GDPR의 일부 규정에 대해서는 회원국의 별도 입법이 요구되므로, 기업들은 각 회원국의 개인정보 보호 관련 입법 동향에 대해 지속적인 모니터링 필요[6]

□ 과거에는 회원국 간 개인정보 보호법제가 달라 기업 활동에 제약이 있었지만, GDPR 제정으로 보다 강력하고 일관성 있는 규제 가능

다. 체계

□ GDPR은 전문(Recital) 173개 조항, 본문 총 11장 9개조로 구성, 기존 지침이 총 7장 34개조로 구성된 것에 비해 내용이 대폭 증가

표 III-1. GDPR의 체계

전문(Recital) 173개 조항	
본문 **11장(Chapter)** **99개 조항(Article)**	제1장 일반규정 (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 협력 및 일관성 (Co-operation and Consistency)
	제8장 구제책, 책임, 처벌 (Remedies, Liability and Sanctions)
	제9장 특정 정보처리 상황에 관한 규정 (Provisions Relating to Specific Data Processing Situations)
	제10장 위임법률 및 시행법률 (Delegated Acts and Implementing Acts)
	제11장 최종규정 (Final Provisions)

자료: European Union(2016).

6) GDPR은 과징금(administrative fines)의 대상이 되지 않는 위반 사항에 대해 각 회원국이 별도의 입법을 하도록 규정(제84조제1항)

라. 적용 대상 및 범위(제1~4조)

1) 적용 대상 개인정보

□ **IP 주소 등 온라인 식별자(online identifier) 정보**가 개인정보에 포함되는 등 이전 지침에 비해 개인정보의 정의가 구체적으로 제시됨.

○ 개인정보는 식별되었거나, 식별가능한 자연인(정보주체)과 관련된 모든 정보

– 자연인을 직간접적으로 식별가능한 경우라면, 이름·전화번호 등 일반적인 개인정보 외에 온라인식별자나 위치정보도 개인정보에 해당*

* 예: IP 주소, 온라인 쿠키(cookie)를 통해 개인 식별이 가능한 경우 온라인 식별자에 해당

□ **가명화 정보**는 추가 정보를 이용하여 개인을 식별할 수 있는 정보로서 개인정보로 간주되어 GDPR의 적용 대상이 되지만, 익명화하여 더 이상 식별할 수 없는 정보는 적용 대상에서 제외

○ 가명화(pseudonymisation)는 추가적인 정보의 사용 없이는 특정 정보주체를 식별할 수 없는 방식으로 수행된 개인정보의 처리를 의미

○ 가명정보를 이용하기 위해서는 추가적인 정보를 분리 보관하고, 해당 정보를 통해 자연인을 식별하지 않도록 기술·조직적 조치(technical and organizational measures)를 취해야 함.

□ 적용대상이 되는 **민감정보**는 “특별한 유형의 개인정보(special categories of personal data)”로서, 인종·민족, 정치적 견해, 종교·철학적 신념, 노동조합 가입 여부, 유전자 또는 생체정보*, 건강, 성생활 또는 성적 취향의 정보를 지칭

* 유전정보와 바이오정보 등 포함

○ 민감한 개인정보는 정보주체가 명시적으로 동의 의사를 표현한 경우를 제외하고는 원칙적으로 처리가 금지됨.

□ **살아있는 자연인의 개인정보에 적용**되나, 회원국이 사망자의 개인정보 처리와 관련된 규정을 별도로 두는 것은 제한하지 않음.

○ 법인과 법인으로 설립된 사업체의 이름, 법인의 형태, 연락처 등에 대한

처리에는 적용되지 않음.

□ **자동화된 수단(automated means)에 의한 개인정보 처리에 적용되지만,** 수기처리라 하더라도 파일링시스템의 일부를 구성하는 경우 적용 대상이 됨.

2) 적용 대상 주체

□ **컨트롤러와 프로세서 모두에게 적용**되며, 특히 **프로세서에게 개인정보의 처리활동 기록 등 구체적인 법적 의무 부과**

표 Ⅲ-2. 컨트롤러와 프로세서의 정의와 역할

구분	정의
컨트롤러	• 개인정보의 처리 목적 및 수단을 단독 또는 제3자와 공동으로 결정하는 자연인, 법인, 공공기관(public authority), 에이전시(agency), 기타 단체(other body)를 의미 • 이러한 처리의 목적 및 수단이 EU 또는 회원국 법률에 의해 결정되는 경우, 컨트롤러의 지명 또는 지명을 위한 특정 기준은 EU 또는 회원국 법률에서 규정 가능
프로세서	• 컨트롤러를 대신하여 개인정보를 처리하는 자연인, 법인, 공공 기관(public authority), 에이전시(agency), 기타 단체(other body)를 의미

자료: European Union(2016).

□ **EU 역내에 거점(establishment)을 가지고 있고, 해당 사업장에서 영위하는 활동에 개인정보가 포함되면 GDPR 적용**

○ '거점'이 구체적으로 정의되어 있지 않지만, 일정한 조치(stable arrangement)를 통해 효과적이고 실질적인 활동(effective and real exercise of activity)을 수행하는 경우를 의미하며, 그 형태가 지점(branch) 혹은 자회사(subsidiary)이건 관계없음.

□ **EU에 거점을 가지고 있지 않더라도, ① EU내 거주자에게 재화나 서비스를 제공(offering)하는 경우, ② EU내 거주자의 행동을 모니터링 하는 경우 적용**

○ 단순히 인터넷에서 공개했다고 '제공'이라고 단정할 수 없으며, **언어, 통화, 서비스 제공 대상 등을 종합적으로 고려**해야 함.

♣ 재화나 용역을 '제공'한다고 판단할 수 있는 요소 ♣

① 언어: 소재 또는 거주 국가의 고객과 관련 없는 EU 회원국의 언어를 사용
② 통화: 소재 또는 거주 국가에서 일반적으로 사용하지 않는 EU 회원국의 통화를 사용
③ 도메인 이름: 웹사이트 도메인이 EU 회원국의 최상위 도메인 명칭을 사용(예: .de, .fr 등)
④ 회원국 시민 언급: 재화나 서비스를 홍보하기 위해 EU 회원국 시민 언급
⑤ 소비자: EU 내에 높은 비율의 소비자를 보유한 경우
⑥ 광고 타게팅: EU 회원국의 정보주체를 목표로 광고 제공 등

자료: 한국인터넷진흥원(2017)

○ 모니터링은 정보주체의 온라인 활동을 지속적으로 추적(tracking)하는 것을 의미

– 예컨대, 맞춤형 광고의 제공을 위한 이용자 브라우징 정보를 수집, 축적, 분석하는 행위는 모니터링에 해당

○ 정보주체가 실제로 재화·서비스의 비용을 지불했는지 여부와 무관

– 비용 지불과 무관한 개인정보 제공이 매우 빈번한 현실을 반영

□ ① EU 개별 회원국의 형사법 등 EU 법률의 범위를 벗어나거나, ② 개별 회원국의 해외·안보 정책 관련 활동, ③ 자연인의 개인 또는 가사활동, ④ 공공안전 및 범죄예방, 형사처벌 집행 등과 관련된 활동에는 적용되지 않음.

2 GDPR의 내용

가. 원칙

□ 개인정보 처리 원칙(Principles, 제5조)

○ **(적법성, 공정성, 투명성)** 개인정보를 적법하고, 공정하며 투명한 방식으로 처리해야 함.

○ **(목적제한)** 구체적·명시적이며, 적법한 목적을 위해 개인정보를 수집해야 하며, 해당 목적과 부합하지 않는 방식으로 추가 처리해서는 안 됨.

– 다만 공익을 위한 보관 목적, 과학 또는 역사적 연구, 통계 목적을 위한 추가 처리는 최초 목적과 무관하게 가능

○ **(개인정보처리 최소화)** 개인정보의 처리는 적절하며 관련성이 있고, 그 처리 목적을 위해 필요한 범위로 한정되어야 함.

○ **(정확성)** 개인정보의 처리는 정확해야 하고, 필요시 내용을 최신으로 유지해야 하며, 처리 목적에 비추어 부정확한 정보의 즉각적인 삭제·정정을 보장하기 위한 모든 합리적 조치를 취해야 함.

○ **(보관기간 제한)** 필요한 기간이 경과한 후에는 정보 주체를 식별할 수 있는 형태로 개인정보를 보관해서는 안 됨.

○ **(무결성 및 기밀성)** 개인정보는 적절한 기술적·조직적 조치를 통하여, 권한 없는 처리, 불법적 처리 및 우발적 멸실, 파괴 또는 손상에 대비한 보호 등 적절한 보안을 보장하는 방식으로 처리되어야 함.

○ **(책임성)** 컨트롤러는 상기 원칙을 준수할 책임을 지며, 이를 입증(demonstrate)할 수 있어야 함.

□ 처리의 적법성(Lawfulness of Processing, 제6조)

○ GDPR에 따른 적법한 처리가 되려면, **기업은 개인정보 처리 전에 법적 근거를 확인해야 함**(아래 표 참고).

표 III-3. 개인정보 처리를 위해 적용 가능한 적법 처리 근거[7]

관련 조항	내 용
제6조제1항(a)호	정보주체의 동의
제6조제1항(b)호	정보주체와의 계약 이행이나 계약 체결을 위해 필요한 처리
제6조제1항(c)호	법적 의무 이행을 위해 필요한 처리
제6조제1항(d)호	정보주체 또는 다른 사람의 중대한 이익을 위해 필요한 처리
제6조제1항(e)호	공익을 위한 임무의 수행 또는 컨트롤러에게 부여된 공적 권한의 행사를 위해 필요한 처리
제6조제1항(f)호	컨트롤러 또는 제3자의 적법한 이익 추구 목적을 위해 필요한 처리 (단, 정보주체의 이익, 권리 또는 자유가 그 이익보다 중요한 경우는 제외)

자료: European Union(2016)

□ 동의(Consent, 제4조, 제7조, 전문)

○ GDPR에서 동의는 **정보주체가 진술 또는 적극적 행동을 통하여 자신의 개인정보 처리에 대한 의사를 구체적이고 뚜렷하게 표현하는 것**을 의미

○ 동의는 적법한 개인정보 처리 근거 중 하나로서, **명시적 동의 의사는 민감정보의 처리, 프로파일링을 포함한 자동화된 결정 또는 개인정보 역외 이전 관련 처리의 적법한 근거**가 됨.

– 동의 의무 위반 시 전세계 연간 매출액의 4%, 또는 2천만 유로 이하의 과징금 부과(제83조 제5항 a)

○ 동의 거부에 따른 불이익이 없어야 하고, 언제든지 동의를 쉽게 철회할 수 있어야 하며, 이용약관으로부터 동의를 분리하여야 함.

– 전문 제42조는 "정보 주체가 실질적이거나 자유로운 선택권이 없거나, 불이익 없이 동의를 거부하거나 철회할 수 없는 경우, 그 동의는 자유의사로 부여된 것으로 간주되지 않는다"고 명시

○ **모든 동의는 사전에 이루어져야 하며(opt-in consent), 디폴트 세팅(default setting) 또는 미리 체크된 박스는 유효한 동의에 해당되지 않음.**

○ 만 16세 미만의 아동에게 서비스를 제공하는 경우 친권자의 동의를 얻어야 하며, 민감정보 및 자동화된 결정 처리 시 명시적 동의를 받아야 함.

7) 이 조건은 공공기관이 그 임무 수행을 위해 처리한 경우에는 적용되지 않음.

– 각 회원국은 아동 연령기준을 만 13세 미만까지 낮추어 규정 가능

♣ 영국 개인정보 감독기구(Information Commissioner Office: ICO)의 동의 가이드라인 ♣

- 동의 요청은 눈에 잘 띄고, 간결하며, 다른 이용약관과 구분하여 이해하기 쉽도록 해야 함.
- 동의서에는 조직 및 제3자의 이름, 개인정보를 사용하는 목적, 개인정보로 수행할 작업, 그리고 언제든지 동의를 철회할 권한이 포함되어 있어야 함.
- 정보주체가 적극적으로 선택하도록 해야 함. 미리 자동체크 된 동의(pre-ticked box)나 옵트 아웃(opt-out) 및 기본 설정(default setting)을 사용하지 않도록 주의
- 복수의 목적과 다른 유형의 처리에 대해서는 개별적으로 동의하는 세부 옵션 제공
- 동의에 대한 증거자료를 기록으로 보관해야 함.
- 정보주체는 언제든지 쉽게 본인의 동의를 철회할 수 있도록 환경을 설정해야 함.
  ※ 가능하면 동의할 때와 동일한 방법으로 동의 철회가 가능해야 함.
- 동의서를 검토하고 변경 사항이 있을 경우, 새롭게 수정해야 함.

자료: ICO. "GDPR consent guidance" 웹페이지.

□ **민감정보**(Special categories of personal data, **제9조**)[8]

○ **민감정보의 처리는 원칙적으로 금지되나 아래의 경우에 한해 허용**

– 정보주체의 명시적 동의(explicit consent)

– 고용, 사회보호·보장법(social protection and social security) 또는 단체협약(collective agreement) 분야의 의무 이행

– 물리적 또는 법적으로 동의를 할 능력이 없는 정보주체의 중대한 이익 보호

– 정치·철학·종교 목적을 지닌 비영리단체나 노동조합이 수행하는 처리로서, 동의 없이는 제3자에게 공개하지 않는 경우

– 정보주체가 일반에게 공개한 것이 명백한 정보

– 법적 주장의 구성, 행사나 방어 또는 법원의 사법권 행사

– 중대한 공익을 위해서 또는 EU나 회원국 법률을 근거로 하는 처리로서, 추구하는 목적에 비례하며 적절한 보호 조치가 있는 경우

– EU나 회원국 법률 또는 의료 전문가와의 계약을 근거로, 예방 의학이나 직업 의학, 종업원의 업무능력 판정, 의료 진단, 보건·사회복지·치료, 보건이나

8) 민감정보 유형에 유죄 판결 및 형사범죄 정보를 포함시키고 있지 않음.

사회복지시스템의 관리 및 서비스 등의 제공

- 보건에 대한 국경을 넘은 심각한 위협으로부터의 보호, 또는 의료 혜택 및 약품이나 의료 장비의 높은 수준의 확보 등 공중보건 영역에서의 공익 추구
- 공익을 위한 저장(archiving), 과학·역사 연구, 통계 목적

나. 정보주체의 권리 보장

□ GDPR은 삭제권, 개인정보 이동권, 자동화된 결정(프로파일링 포함) 관련 권리 등을 새로 도입하여 정보주체의 권리를 강화

표 III-4. GDPR의 강화된 정보주체 권리

No	정보주체의 권리	관련 조문
1	정보를 제공받을 권리(Right to be informed)	제13조 제14조
2	정보주체의 열람권(Right of access by the data subject)	제15조
3	정정권(Right of rectification)	제16조
4	삭제권(Right of erasure. 잊힐 권리)	제17조
5	처리에 대한 제한권(Right of restriction of processing)	제18조
6	개인정보 이동권(Right to data portability)	제20조
7	반대할 권리(Right to object)	제21조
8	자동화된 결정 및 프로파일링 관련 권리 (Right to related to automated decision making and profiling)	제22조

자료: European Union(2016)

□ 정보를 제공받을 권리(Right to be informed)

○ 컨트롤러는 공정하고 투명한 처리원칙을 보장하기 위해 **정보주체에게 본인의 개인정보 처리에 관한 정보를 어떻게 사용하고 있는지 알려주어야 함.**

○ **정보주체로부터 정보를 직접 수집하는 경우와 그렇지 않은 경우**로 나누어 살펴볼 수 있음(아래 표 참고).

○ 제공시기는 정보 취득 후 합리적인 기간 내(최대 1개월), 또는 개인정보가 정보주체와 연락(communication) 목적으로 이용되는 경우, 늦어도 해당 정보주체에게 최초로 연락한 시점에 이루어져야 함.

표 III-5. 정보주체가 제공받을 수 있는 정보

제공 정보 내용	직접 수집 (취득 시 제공)	직접 수집 x (1개월 이내 등)
컨트롤러 및 (해당되는 경우) 컨트롤러의 대리인과 DPO의 신원과 연락처	O	O
해당 개인정보의 처리 목적 및 처리의 법적 근거	O	O
(해당되는 경우) 컨트롤러 또는 제3자의 정당한 이익	O	O
개인정보의 유형(categories)	-	O
개인정보 수령인(recipient) 또는 수령인의 유형(categories)	O	O
제3국으로 이전한 상세 내용 및 보호방법	O	O
보유기간 또는 보유기간 결정을 위해 적용한 기준	O	O
정보주체의 각 권리의 존재	O	O
(해당되는 경우) 언제라도 동의를 철회할 수 있는 권리	O	O
감독기구에 불만을 신청할 수 있는 권리	O	O
개인정보의 출처 및 공개적으로 접근이 허용된 출처인지 여부	-	O
개인정보의 제공이 법률이나 계약상의 요건이나 의무인지 여부 및 개인정보 제공을 하지 않을 경우 생길 수 있는 영향(possible consequences)	O	-
프로파일링 등 자동화된 결정의 존재 및 어떻게 결정되는 지에 대한 정보와 그 중요성 및 영향	O	O

자료: European Union(2016)

□ 열람권(Right of access)

○ 컨트롤러는 정보주체가 개인정보 처리가 어떻게 이루어지고 있는지를 알고 그 적법성을 확인할 수 있도록, 정보주체의 요구가 있을 경우 늦어도 1개월 이내에 다음의 모든 정보에 대해 열람할 수 있도록 조치해야 함.

- 처리 목적과 관련된 개인정보의 유형
- 개인정보를 제공받았거나 제공받을 수령인 또는 수령인의 범주
- (가능하다면) 개인정보의 예상 보유 기간, 또는 (가능하지 않다면) 해당 기간을 결정하기 위해 이용하는 기준
- 컨트롤러에게 본인의 개인정보에 대한 수정, 삭제 또는 처리 제한이나 처리에 대한 반대를 요구할 수 있는 권리의 유무 등

○ 컨트롤러는 정보주체의 열람 요구에 따른 사본을 무료로 제공해야 하지만,

정보주체의 요구가 명백히 근거가 없거나 반복적인 요구 등 과도하다면 요구를 거부하거나 '합리적 요금'을 부과할 수 있음.

□ 정정권(Right to rectification)

○ 정보주체는 자신의 개인정보가 부정확하거나 불완전하다면 이에 대한 정정을 요구할 권리가 있으며, 컨트롤러는 정보주체의 정정 요구가 있으면 부당한 지체 없이 필요한 조치를 취해야 함.

□ 삭제권(Right to erasure)

○ 정보주체는 본인에 관한 정보의 삭제를 요구할 권리를 가지며, 컨트롤러는 다음 하나에 해당할 경우 정보주체의 삭제권을 보장해야 함.

– 개인정보가 원래의 수집·처리 목적에 더 이상 필요하지 않은 경우

– 정보주체가 동의를 철회한 경우

– 정보주체가 처리에 반대하는 경우로서 처리의 계속을 위한 더 중요한 사유가 없는 경우

– 개인정보가 불법적으로 처리된 경우(GDPR 위반 등) 등

○ 컨트롤러는 다음 중의 하나에 해당될 경우에는 삭제요구를 거부할 수 있음.

– 표현 및 정보의 자유에 관한 권리 행사

– 공익적 임무 수행 및 직무권한 행사를 위한 법적 의무 이행

– 공공보건을 위한 목적 등

□ 처리 제한권(Right to restriction of processing)

○ 컨트롤러는 다음의 하나에 해당될 경우에는 정보주체의 개인정보 처리 제한 요구를 이행해야 함.

– 정보주체가 개인정보의 정확성에 이의를 제기한 경우(개인정보의 정확성을 입증할 때까지 처리 제한)

– 처리가 불법적이며, 정보주체가 삭제를 반대하고 대신 개인정보의 처리제한을 요구한 경우

– 더 이상 개인정보가 필요하지 않지만 정보주체가 법적 청구권의 수립, 행사 또는 방어를 위해 그 정보를 요구한 경우 등

○ 개인정보의 처리가 제한된 경우에도 불구하고 다음 하나에 해당되는 경우에는 처리할 수 있음.

– 정보주체의 동의가 있는 경우, 법적 청구권의 입증이나 행사·방어를 위한 경우, 제3의 자연인이나 법인의 권리 보호를 위한 경우 등

□ **개인정보 이동권**(Right to data portability)[9)]

○ 정보주체는 개인정보를 다른 서비스에 재사용할 수 있도록 개인정보의 이동을 요구할 수 있는 권리를 지님.

– 컨트롤러에게 제공한 자신에 관한 개인정보를 체계적으로 구성되고, 일반적으로 사용되며 기계 판독이 가능한 형식으로 제공 받거나, 그 정보를 다른 컨트롤러에게 제공할 것을 요구할 수 있는 권리

○ 정보주체는 컨트롤러에게 제공한 자신에 관한 개인정보를 제공받을 권리가 있으며, 다음의 경우에 적용

– 정보주체가 컨트롤러에게 제공한 개인정보로서, 처리의 근거가 정보주체의 동의나 계약 이행으로서, 자동화된 수단에 의해 처리되는 경우

○ 컨트롤러가 정보주체의 개인정보 이동권을 위하여 개인정보를 제공할 때에는 상호운용성(interoperability)을 보장할 수 있도록 다음 사항을 고려해야 함.

– 구조적이며 보편적으로 사용되는 기계판독이 가능한 형태[10)]로 제공

– 무료 제공

9) 개인정보를 여러 다른 서비스에서 재사용할 수 있도록 정보주체가 개인정보 처리자에게 정보의 이동을 요구할 수 있는 권리로서, 자신의 정보를 개인정보 처리자로부터 수령하거나 해당 정보를 다른 처리자에게 전송할 수 있도록 하는 권리를 의미함. 개인정보 이동권 도입의 목적은 ▲온라인 서비스에 대한 정보주체의 선택권을 확대하고 ▲디지털 시장에서 데이터에 대한 독점 가능성을 완화함으로써 기업 간 공정한 경쟁 환경 조성으로 요약할 수 있음.

10) 정보의 특정 요소를 소프트웨어가 추출할 수 있도록 구조화한 것

– 정보주체의 요구가 있고, 또한 기술적으로 가능하다면 해당 개인정보를 한 컨트롤러에서 다른 컨트롤러로 직접 전송

○ 개인정보 이동권으로 인해 지재권이나 영업비밀 등 타인의 권리와 자유가 침해되는 경우에는 해당 의무가 적용되지 않음.

□ **반대권**(Right to object)

○ 정보주체는 프로파일링 등 본인과 관련한 개인정보의 처리에 대해 반대할 권리를 가지며, 컨트롤러는 특별한 사유가 없는 한 개인정보의 처리를 중단하는 등 관련 조치를 취하여야 함.

○ 다음의 정당한 처리에 대해서도 정보주체가 반대할 권리 보장

– 컨트롤러의 정당한 이익 또는 공익적 임무 수행 및 직무권한 행사에 근거한 개인정보의 처리

– 과학적, 역사적 연구 및 통계 목적의 처리

○ 직접 마케팅(프로파일링 포함)에 대해서도 반대권 보장

□ **자동화된 결정 및 프로파일링 관련 권리**(Right to related to automated decision making and profiling)

○ 프로파일링은 '개인의 사적인 측면의 평가, 특히 다음 사항의 분석이나 예측을 위한 모든 형태의 자동 처리'(제4조 제4항)

– 직장 내 업무 수행(performance at work), 경제적 상황(economic situation), 건강(health), 개인적 취향(personal preferences), 신뢰성(reliability), 행태(behavior), 위치(location) 또는 이동경로(movements)

○ 정보주체는 ① 법적 효력을 초래하거나 ② 이와 유사하게 본인에게 중대한 영향을 미치는 사항에 대하여 프로파일링 등 자동화된 처리에만 근거한 결정의 적용을 받지 않을 권리를 가짐.

○ 컨트롤러는 정보주체가 아래 사항을 요구할 수 있도록 보장해야 함.

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

○ 프로파일링 등 자동화된 결정이 다음 중 하나에 해당될 경우에는 정보주체의 권리가 적용되지 않음.

- 컨트롤러와 정보주체 간의 계약의 체결이나 이행, 사기나 탈세 방지 목적 등 법에 의하여 인정된 경우, 명시적 동의에 근거한 경우

다. 컨트롤러와 프로세서의 일반적인 의무

□ 컨트롤러의 책임(Responsibility of the controller)

○ 컨트롤러는 개인정보 처리의 성격, 범위, 목적, 위험성 등을 고려하여 개인정보의 처리가 GDPR을 준수하여 수행되는 것을 보장하고 입증할 수 있는 적절한 기술·조직적 조치를 이행해야 함(제24조).

○ 둘 이상의 컨트롤러가 공동으로 개인정보 처리 목적과 수단을 정하는 경우 공동 컨트롤러가 되며, 당사자 간의 합의를 통해 정보주체의 권리보장 등 GDPR에 따른 책임에 대해 각자의 의무를 투명하게 결정해야 함(제26조).

□ 프로세서(Processor, 제28조, 제29조)

○ 프로세서는 컨트롤러의 특정(specific) 또는 일반(general) 서면 승인 없이는 다른 프로세서가 업무를 관여하게 할 수 없음.

○ 컨트롤러는 개인정보 처리가 GDPR을 준수하고, 정보주체의 권리를 보호하는 적절한 기술·조직적 조치를 이행한다는 충분한 보증을 제공하는 프로세서만 활용해야 함.

○ 프로세서의 의무는 다음과 같음.

- 원칙적으로 컨트롤러의 문서화된 지시에 의해서만 처리

- 관련 개인정보를 처리하는 자에게 기밀 준수를 약속하거나, 또는 실정법상 기밀준수 의무를 지고 있음을 보장

- 개인정보 처리의 보안을 위해 요구되는 모든 조치를 취해야 함.
- 다른 프로세서의 지정과 관련한 규정 준수
- 컨트롤러가 정보주체의 개인정보 권리를 보장하기 위해 필요한 조치에 있어 지원 활동을 이행할 것
- 회원국 개인정보 보호당국의 승인을 받기 위한 컨트롤러의 활동 지원
- 컨트롤러와의 관계 종료 시, 컨트롤러의 선택에 따라 개인정보를 반환 또는 파기[11)]
- GDPR 준수여부를 입증하기 위해 필요한 모든 정보를 컨트롤러에게 제공
- 컨트롤러 또는 컨트롤러가 위임한 자가 수행하는 감사를 받아야 하며, 컨트롤러의 지시가 GDPR 또는 기타 회원국의 개인정보 보호 규정을 위반한다고 판단되는 즉시 컨트롤러에게 통지해야 함.

○ 프로세서가 처리의 목적 및 수단을 결정함으로써 GDPR을 위반하는 경우, 프로세서는 해당 처리와 관련하여 컨트롤러로 간주됨.

□ 컨트롤러 또는 프로세서의 대리인(Representatives, 제27조)

○ EU 내에 설립되지 않은 컨트롤러 또는 프로세서는 EU 역내 대리인을 서면으로 지정해야 하지만(제3조 제2항), 다음의 경우는 예외

- ① 해당 처리가 간헐적으로 발생하고, ② 대규모의 처리가 아니면서, ③ 민감정보 또는 유죄 판결 및 형사범죄에 관련된 개인정보의 처리를 포함하지 않으며, ④ 개인정보 처리의 성격·상황·범위·목적을 고려했을 때 개인의 권리와 자유에 대한 위험을 초래할 가능성이 낮은 경우
- 공공 기관·기구의 경우(public authority or body)

○ 대리인은 개인정보가 처리되거나 정보주체의 행동이 모니터링되는 회원국 중 한 곳에 설립되어야 함.

11) 단, EU 또는 회원국 법률이 해당 개인정보의 보관을 요구하는 경우는 예외

라. 기업 책임성 강화

□ 개인정보 처리활동의 기록(Records of processing activities, 제30조)

○ 종업원 250인 이상의 기업은 개인정보 처리활동에 대한 기록을 의무적으로 문서화하고 보유해야 함.

○ 해당 기업이 수행하는 개인정보의 처리가 다음 중 하나에 해당하는 경우, 종업원 수와 무관하게 개인정보 처리활동의 기록이 필요

– 정보주체의 권리와 자유에 위험을 초래할 가능성이 있는 개인정보 처리, 또는 민감정보 처리, 또는 범죄경력 및 범죄행위에 관련된 개인정보 처리

○ 다음의 내용이 포함된 개인정보 처리활동을 기록·보유해야 함.

– 컨트롤러의 성명과 연락처, 처리 목적, 정보주체 및 개인정보의 유형(categories), 개인정보 수령인의 유형, 제3국 이전 시 국외이전 방식에 대한 체계(mechanism)와 보호 조치(safeguards), 보유기간, 기술·조직적 보호조치에 대한 설명 등

□ 개인정보 보호 적용설계 및 기본설정(Data protection by design and by default, 제25조)

○ 컨트롤러는 최신기술, 비용, 처리의 성격과 범위·상황·목적·개인정보 처리로 인한 개인의 권리와 자유의 위험성을 고려하여 처리 방법 결정 단계와 처리 과정 상에서 적절한 기술·조직적 조치를 이행해야 함.

– 이러한 조치에는 개인정보처리의 최소화(data minimisation), 처리에 필요한 보호조치(safeguards), 가명화(pseudonymisation) 등이 해당

– 모든 프로젝트의 초기단계부터 개인정보 보호를 중요한 고려사항으로 하고, 라이프사이클에서 전반에 걸쳐 개인정보를 보호한다는 취지

– 개인정보 보호 적용설계 및 기본설정은 공개입찰(public tenders)에서도 고려(전문 제78조)

○ 컨트롤러는 기본설정을 통해(by default) 정해진 목적 내에서 개인정보가 처리될 수 있도록 적절한 기술·조직적 조치를 이행해야 함.

- 이 의무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보유기간 및 접근 가능성(accessibility)에 대해 적용

□ 개인정보 영향평가(Data protection impact assessment, 제35조 등)

○ 컨트롤러는 새로운 기술을 사용하고 그 처리 유형이 개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우, 개인정보를 처리하기 이전에 예상되는 개인정보 처리에 대한 영향평가를 수행해야 함.

- 기업이 개인정보 처리 관련 문제점을 조기에 발견·해결하여 리스크를 줄일 수 있는 수단으로 간주

○ 개인정보 영향평가에는 특히 위험을 완화하고 개인정보 보호를 보장하며 GDPR 준수를 입증하기 위한 조치가 포함되어야 함.

○ 특히, 다음 중 하나의 경우에는 개인정보 영향평가를 수행해야 함.

- 프로파일링을 포함한 자동화된 처리에 근거한 자연인에 대한 체계적이고 광범위한 평가로서, 이에 기초한 결정이 해당 정보주체에게 법적 효력을 미치거나 중대한 영향을 미치는 경우

- 민감정보 또는 유죄 판결 및 형사범죄에 대한 대규모 처리

- 공개적으로 접근 가능한 장소에 대한 대규모의 체계적 모니터링(예: CCTV)

○ 감독기구(supervisory authority)는 영향평가 대상이 되는 처리작업 리스트 공개

○ 영향평가 결과 고위험이 예상되는 경우 컨트롤러는 해당 처리 작업에 앞서 감독기구에 자문을 구해야 함(prior consultation).

□ DPO(Data Protection Officer) 지정(제37~39조)

○ 컨트롤러와 프로세서는 다음 경우에 필수적으로 DPO를 지정해야 함.

- 공공기관(사법적 권한을 행사하는 법원은 예외)

- 컨트롤러 또는 프로세서의 “핵심활동”이 정보주체에 대한 “대규모”의 “정기적이고 체계적인 모니터링”이거나,

– 민감정보나 범죄경력 및 범죄행위의 “대규모” 처리

○ DPO는 내부인 또는 서비스 계약을 통한 외부인으로 선임할 수 있으며, 다음의 임무 수행

– 컨트롤러, 프로세서 및 임직원에게 GDPR 및 다른 정보보호 법규의 준수의무를 알리고, 관련 법규 이행상황 모니터링

– 컨트롤러 또는 프로세서에게 정보 제공, 조언 및 권고사항 제시

– 개인정보 영향평가에 대한 자문 및 평가 이행 감시

○ 기업은 DPO에게 개인정보 접근 및 처리 작업 등을 수행하고, 전문 지식을 유지하는 데 필요한 자원을 제공함으로써 DPO를 지원해야 함.

○ 고용주는 DPO에 대해 다음과 같은 권한을 부여해야 함.

– 기업 조직의 최고 경영층, 즉 이사회에 보고할 수 있도록 할 것

– 독립적으로 임무를 수행하며, 임무수행으로 해고나 불이익을 당하지 않을 것

– GDPR의 의무이행을 위해 적절한 자원을 제공할 것

○ DPO는 GDPR을 준수하지 않은 데 대해 개인적 책임을 지지 않음.

– DPO가 아니라, 컨트롤러 또는 프로세서가 GDPR을 준수하여 개인정보를 처리했다는 것을 보장하고, 이를 입증할 수 있는 적절한 기술조직적 조치를 이행해야 함.[12)]

□ **행동강령 및 인증제도(Codes of conduct & Certification mechanism, 제40~42조)**

○ 기업의 GDPR 준수 입증, 투명성과 책임성 보장, 제3자에 대한 개인정보 보호 수준의 척도로서 승인된 행동강령과 인증제도 활용 가능

○ 회원국과 감독기구, EU 집행위원회는 행동강령의 작성을 장려해야 하고, 협회나 대표단체가 행동강령을 작성할 수 있음.

– 행동강령은 분야별 특성, 중소·중견기업의 특수한 니즈를 고려

12) Article 29 Data Protection Working Party(2016).

- 정보주체를 포함한 이해관계자들과 협의를 통해 작성하여 감독기구의 승인을 받아야 함.

○ 기업은 인증 제도를 통해 기술적·조직적 조치를 실시하고 있음을 보여줄 수 있으며, 정보 이전의 적절성과 관련된 보호조치를 실시하고 있음을 입증할 수 있음.[13]

마. 개인정보 침해 발생 시 조치사항

□ 감독기구에 대한 통지(제33조)

○ 개인의 권리와 자유에 위험을 야기할 수 있는 침해, 즉 차별행위, 평판훼손, 재정적 손실, 비밀의 누설 또는 다른 중대한 경제적·사회적 불이익 등의 경우가 발생할 경우 감독기구에 통지해야 함.

○ 컨트롤러는 개인정보 침해 인지 후 가능한 72시간 이내에 관련 감독기구에 통지하여야 하며, 다음의 내용을 포함해야 함.

- 침해 관련 정보주체 및 개인정보 기록의 범주 및 대략적인 개수 등 개인정보 침해 성격
- DPO 및 다른 연락처에 대한 이름과 상세 연락처
- 개인정보 침해로 발생할 수 있는 결과
- 침해로 발생 가능한 부작용을 완화하는 조치 등 해당 개인정보 침해 해결을 위해 컨트롤러가 취하거나 취하도록 제시된 조치

□ 정보주체에 대한 통지(제34조)

○ 컨트롤러는 개인정보의 침해가 개인의 권리와 자유에 관해 높은 위험을 초래할 가능성이 있는 경우, 정보주체가 필요한 예방조치를 취할 수 있도록 해당 정보주체에게 직접 통지해야 함.

○ 정보주체에게 통지 시 개인정보 침해의 성격을 명확하고 평이한 언어로 설명

13) 인증의 최대 유효기간은 3년이며, 인증의무를 더 이상 충족하지 않을 경우 인증은 철회될 수 있음.

하여야 하며, 최소한 다음의 정보가 포함되어야 함.

- DPO 및 다른 연락처의 성명 및 상세 연락처
- 개인정보 침해로 발생할 수 있는 결과
- 침해로 발생 가능한 부작용을 완화하는 조치 등 해당 개인정보 침해 해결을 위해 컨트롤러가 취하거나, 취하도록 제시된 조치

바. EU 역외로의 개인정보 이전

□ **GDPR 규정에 부합할 경우에만 EU 밖으로 개인정보 이전 가능**(제44~47조)

○ **적정성 평가**(Adequacy Decision), **표준 계약**(Standard Clauses), **구속력 있는 기업 규칙**(BCRs, Binding Corporate Rules), **승인된 행동강령**(Code of Conduct) **및 인증제도**(Certificate) **등**의 방법으로 가능

○ 同규정의 취지는 GDPR이 규정하는 개인정보 보호 수준이 역외에서도 유지되도록 보장하는 것

○ 역외로 이전한 정보를 제3국으로 다시 이전하여 처리할 경우에도 적용

□ **적정성 평가에 따른 이전**(Transfer on the basis of an adequacy decision)

○ 유럽집행위원회가 적정한 보호수준을 보장한다고 판정한 경우, 해당 국가 또는 국제기구로의 개인정보 이전 가능

- 즉, EEA 및 EU에 의해 안전하다고 분류된 국가로의[14] 이전에는 일반적으로 별도의 보호조치가 요구되지 않음.
- 미국으로 이전하는 경우, 해당정보를 이전 받는 자가 Privacy Shield에 등록된 경우 역외 이전이 가능[15]

○ 최소 4년마다 정기적인 검토(periodic review) 실시[16]

14) 안도라, 아르헨티나, 캐나다, 페로 제도, 건지 섬, 이스라엘, 만 섬, 저지, 뉴질랜드, 스위스, 우루과이, 미국 등 12개국이 적정성 평가 승인을 받음.
15) 기업의 Privacy Shield 등록 여부는 https://www.privacyshield.gov/list에서 확인할 수 있음.
16) 유럽집행위원회는 적정성 결정을 폐지.개정 또는 정지할 수 있는 권한을 가짐.

♣ EU 적정성 평가의 고려 요소(GDPR 45조 2항) ♣

- 법치 수준, 인권 및 기본적 자유의 존중, 공공안전·국방·국가안보, 형사법, 공공기관의 개인정보에 대한 접근 등 관련 법규; 국외 데이터 이전을 포함한 관련법의 이행 수준; 정보 주체 보호의 실효성과 강제력, 행정·사법적 배상의 실효성
- 독립성 있는 감독기구의 존재와 기능의 실효성; 데이터 보호 법규 준수의 보장·강제에 대한 책임성
- 관련 국제 협약 가입 여부

자료: European Union(2016).

□ 적절한 보호조치(Appropriate safeguards)에 의한 이전

○ 컨트롤러나 프로세서가 ① 적절한 보호조치를 취하고, ② 정보주체가 행사할 수 있는 권리와 ③ 유효한 법적 구제수단을 보장할 경우 타국가 또는 국제기구에 개인정보 이전 가능

○ 다음과 같은 적절한 보호조치를 구비할 경우 감독기구의 승인 없이 개인정보의 역외 이전 가능

- **법적 구속력과 강제력 있는 장치를 통한 공공기관·기구 간 이전**
- **구속력 있는 기업 규칙**(binding corporate rules)*에 근거한 이전
  * 기업 내부 이전 시 활용되는 수단으로서 주로 대기업에 적용
- **유럽 집행위원회가 제시한 표준 개인정보보호 조항**(standard data protection clauses)[17]에 근거한 이전*
  * 표준 개인정보보호 조항을 토대로 하는 이전을 감독기구에 통지하거나 승인을 받아야 하는 기존 절차는 폐지됨.
- **감독기구가 채택하고 집행위원회가 승인한 표준 개인정보보호 조항**(standard data protection clauses)에 근거한 이전
- GDPR 제40조에 따른 **승인된 행동강령**(approved code of conduct)에 의한 이전

17) 다음의 유럽집행위원회의 Decision에 첨부된 계약서를 사용할 경우 적절한 수준의 안전장치가 구비된 것으로 간주함. COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive95/46/EC of the European Parliament and of the Council (notified under document C(2010)593)(2010/87/EU)

- GDPR 제42조에 따른 **승인된 인증제도(approved certification)**에 의한 이전[18]

○ 다음의 경우 감독기구의 승인이 필요

- 컨트롤러나 프로세서와 외국·국제기구의 컨트롤러, 프로세서 또는 개인정보 수령인 간의 계약 조항(contractual clauses)
- 공공기관·기구 간에 체결된 행정 합의(administrative arrangement)에 삽입된 강제력·실효성 있는 정보주체의 권리 규정

□ 특정 상황에서 상기조건의 충족 없이 국외 이전 가능((제49조. 다음 글상자 참고)

○ 단, 예외조항은 좁게 해석될 가능성이 높은바, 대량의 개인정보를 구조적·지속적으로 전송할 경우 예외조항 적용이 쉽지 않을 것으로 판단됨.

♣ EU 역외 개인정보 이전이 예외적으로 가능한 경우 ♣

- 정보주체가 적정성 평가 및 적절한 보호조치가 없음으로 인해 정보주체에 발생할 수 있는 위험을 고지 받은 후에 명시적으로 이전에 동의(explicit consent)한 경우
- 정보주체와 컨트롤러간의 계약 이행을 위해 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위해 정보이전을 해야 하는 경우
- 정보주체의 이익을 위해 컨트롤러와 기타의 개인이나 법인 간에 체결된 계약의 이행을 위해 정보이전을 해야 하는 경우
- 중요한 공익상의 이유로 정보이전이 반드시 필요한 경우
- 법적 권리의 확립, 행사, 수호를 위해 정보이전이 필요한 경우
- 정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우, 정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위해 정보이전이 필요한 경우
- EU 또는 회원국 법률에 따른 정보 공개 목적, 또는 정당한 목적에 따른 일반국민 또는 제3자의 참조(조회) 목적으로 만들어진 개인정보기록부로부터 EU 또는 회원국 법률에 명시된 조건이 충족되는 범위 내에서 개인정보를 이전하는 경우

자료: European Union(2016).

사. 피해구제 및 제재 규정

□ 구제제도(Remedies)

○ 감독기구에 민원을 제기할 권리(제77조)

18) 행동강령과 인증제도의 주요 내용은 '라. 기업 책임성 강화' 참고.

– 모든 정보주체는 기존의 행정적 또는 사법적 구제를 받을 권리를 제한 또는 침해받지 않고 감독기구에 민원을 제기할 권리가 있음.

– 이 경우 정보주체는 거주지, 근무지 또는 침해 발생이 있을 것으로 추정되는 장소가 소재한 회원국의 감독기구에 민원을 제기할 수 있음.

– 민원접수감독기구는 민원처리 경과와 결과를 민원인에게 알려야 함.[19]

○ 감독기구의 결정에 반하는 사법 구제(제78조)

– 각 자연인 또는 법인은 감독기구의 법적 구속력 있는 결정에 반대하는 사법 구제를 구할 권리가 있음.

○ 컨트롤러 또는 프로세서에 대한 사법 구제권(제79조)

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

– 컨트롤러 또는 프로세서를 상대로 한 법적 절차는 해당 컨트롤러 또는 프로세서의 거점(establishment)이 있는 회원국의 법정에서 진행되어야 함.

□ **손해배상권 및 책임(Right to compensation and liability, 제82조)**

○ 컨트롤러와 프로세서의 손해배상 의무

– GDPR 위반으로 금전·비금전적 손실(pecuniary and non-pecuniary loss)을 입은 자는 컨트롤러 또는 프로세서에게 손해배상을 받을 권리가 있음.

– 개인정보 처리에 관여하는 컨트롤러는 위법한 정보처리로 인해 발생한 피해에 대해 책임 부담

– 프로세서 자신 또는 서브 프로세서의 개인정보처리와 관련하여 GDPR에 명시된 의무 위반 또는 컨트롤러의 지시사항 위반으로 발생한 손해에 대해 책임 부담

– 동일한(하나의) 개인정보의 처리에 복수의 컨트롤러 또는 프로세서가 관여하여 손해가 발생한 경우, 관여한 모든 당사자는 발생한 손해 전체에 대해

19) 기존 지침에 따르면 감독기구는 제기된 민원 관련 개인정보 처리의 적법성을 점검하고, 그 점검 사실을 정보주체에게 통지하는 의무만 부담하였으나, GDPR에서는 민원 처리 경과 및 결과, 그리고 사법적 구제 가능성을 민원인에게 알려야 한다는 점에서 정보주체의 권리가 강화됨.

책임 부담

○ 프로세서의 손해배상 의무

- GDPR에서 규정한 프로세서의 의무를 준수하지 않은 경우
- 컨트롤러의 합법적인 지시에 반한 행위의 경우
- 컨트롤러의 합법적인 지시의 범위를 벗어난 행위의 경우

□ **과징금**(Administrative fines, 제83조)

○ 심각한 위반의 경우, 전 세계 연간 매출액 4% 또는 2천만 유로 중 높은 금액을 과징금으로 부과

○ 일반 위반의 경우, 전 세계 연간 매출액 2% 또는 1천만 유로 중 높은 금액을 과징금으로 부과

○ 과징금의 부과 여부 및 금액에 대한 결정 권한은 회원국 감독기구에 부여

□ **처벌**(Penalties, 제84조)

○ **EU 회원국의 법률상의 차이로 인해 상이한 수준의 처벌이 존재할 것으로 예상**되며, GDPR 위반 시 개별 회원국이 사법 제재를 규정할 수 있어 컨트롤러 또는 프로세서에게 직접적인 처벌이 이루어질 수도 있음.

○ EU 회원국은 GDPR에 따라 각국 법률에 반영하는 조치들을 2018년 5월 25일까지 EU 집행위원회에 통보해야 하므로, 개별 회원국이 어떤 사법 제재를 마련하는지 모니터링 필요

표 III-6. 요약: GDPR 시행에 따른 주요변화

	넓은 영토적 적용 범위
1	EU 내에 설립된 기관의 개인정보 처리 활동 외에, 1) EU 밖에서 EU에 있는 정보주체에게 재화나 용역을 제공하거나, 2) EU내에 있는 정보 주체가 수행하는 활동을 모니터링하는 기관에 적용 ※ 1, 2의 경우 제27조에 의거, EU 회원국에 대리인을 지정해야 함.
	제재규정 강화
2	사업체 그룹의 매출 기반으로 과징금을 부과하며 1) 심각한 위반의 경우 직전 회계연도의 전세계 매출액 4% 또는 2천만 유로 가운데 더 큰 금액, 2) 일반적 위반의 경우 직전 회계연도의 전세계 매출액 2% 또는 1천만 유로 가운데 더 큰 금액으로 정함.
	개인정보의 정의 확대
3	IP 주소, 쿠키, RFID 등이 개인정보인 '온라인 식별자'에 포함되며(전문 제30조), 위치정보는 개인정보의 한 유형으로 간주함. 또한 민감한 성격의 개인정보를 "특별한 유형(special categories)"의 개인정보로 정의하고, 여기에 유전정보와 바이오 정보를 포함. 개인정보의 가명처리(pseudonymisation) 개념을 도입, 이를 적용하는 경우 Data Protection by Design and Default 의 이행 등 다양한 실익을 거둘 수 있게 제도화
	프로세서에게도 다수의 규정이 직접 적용
4	Data Protection Directive 95/46/EC 와는 달리 프로세서를 직접 규제하는 내용을 다수 포함. 프로세서는 적절한 문서화 의무(제30조), 적절한 보안 기준 적용(제32조), 정기 개인정보영향평가 수행(제32조), 개인정보 국외전송 기준 준수(제5장), 국가 감독기구 협조의무(제31조) 등의 의무를 부담. 또한, 프로세서는 제재의 직접적 적용대상이 되며(제83조), GDPR 요구사항을 충족하지 못할 경우 정보주체로부터 배상을 요구 받을 수 있음(제79조).
	개인정보 처리 원칙 확립
5	개인정보를 처리하는 경우 1) (처리) 적법성, 공정성, 투명성 원칙, 2) (수집) 목적 제한의 원칙, 3) 개인정보 최소화 원칙, 4) 정확성 원칙, 5) 저장 제한 원칙, 6) 무결성 및 기밀성 원칙(이상 제5조)을 모두 준수해야 함. 컨트롤러는 이와 같은 원칙을 준수함을 증명(demonstrate compliance) 해야 하는 의무(책임성 원칙 accountability principle)를 부담함.
	적법 처리 기준의 상향
6	개인정보의 (처리) 적법성, 공정성, 투명성 원칙에 따라 개인정보의 처리는 법률에서 허용한 어느 하나 이상의 요건에 해당해야 적법 처리로 인정
	개인정보 국외이전 메커니즘 확립
7	개인정보 국외이전은 적정성 평가(Adequacy Decision) 또는 **[적절한 보호조치 제공 + 정보주체 권리 행사 가능 + 효과적인 법적 구제수단 존재]**의 경우에만 가능. 적절한 보호조치에는 구속력 있는 기업 규칙(BCR), 표준계약서가 있으며, 1) 승인된 행동강령, 2) 승인된 인증제도를 새롭게 추가
	개인정보 유출통지 제도의 도입
8	컨트롤러는 개인정보 유출 사실을 알게 된 때부터 가능한 경우 72시간 내에 감독당국에 신고해야 하며, 정보주체의 자유와 권리에 高위험(high risk)이 예상될 때는 유출 사실을 정보주체에게 통지해야 함. 프로세서는 개인정보 유출 사실을 알게 된 때 컨트롤러에게 알려야함.
	정보주체의 권리 확대
9	컨트롤러의 투명성 의무에 더하여, 정보주체는 열람권(제15조), 정정권(제16조), 삭제권(제17조), 처리 제한권(제18조), 개인정보 이동권(제20조), 반대권(제21조), 프로파일링을 포함한 자동화된 처리 결과를 적용받지 않을 권리(제22조) 등의 권리를 가짐.
	DPO의 의무 지정
10	공공기관(public authorities)이거나, 컨트롤러나 프로세서의 핵심 활동이 1) 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링에 해당하거나, 2) 민감정보나 범죄경력 및 범죄 행위에 대한 대규모 처리인 경우 DPO를 의무적으로 지정해야 함.
	책임성과 거버넌스 강화
11	1) 처리 활동의 세부 기록 유지(제30조), 2) 高위험 처리에 대한 개인정보영향평가 수행(제35조), 3) DPO 지정(제37조), 4) 개인정보 유출통지 및 종합적 기록 유지(제33~34조), 5) Data Protection by Design and Default 이행(제25조) 등 개인정보 처리에 대한 책임성 및 거버넌스 강화
	One Stop Shop 도입
12	컨트롤러, 프로세서는 주사업장 또는 단일사업장에 대한 선임감독기구에 의해 규율됨(제56조). 단, 선임감독기구는 다른 연관 기관과 협력해야 하며, 다른 기관이 특정 사안에 관여할 수 있음.

자료: 행정안전부·한국인터넷진흥원(2017b).

3 주요국 정부의 대응

가. 영국

□ 관련 법령 개정

○ **EU 탈퇴 결정 이후에도 GDPR을 데이터보호법(Data Protection Act)에 반영**하기 위해 2018년 5월 시행을 목표로 데이터보호법 개정 진행

– 기존 법을 대체하여 정보주체가 자신의 개인정보를 더욱 강력하게 통제할 수 있도록 하고 디지털시대의 데이터 보호 프레임워크 보장

– 데이터 접근, 이전, 삭제 권리 등 강화

– 정보위원회(Information Commissioner Office: ICO)의 과징금 부과 권한을 강화하고, 금액을 1,700만 파운드 또는 전세계 매출의 4%로 상향하여 GDPR 규정과 부합

○ 영국의 EU 탈퇴(Brexit)는 GDPR 시행 준비에 영향을 주지 않을 전망

– 금융, ICT 산업 등의 유럽내 위상을 유지하기 위한 대응

□ **정보위원회의 GDPR 관련 가이드 개발 및 이행조치**

○ GDPR에 대한 개괄적 지침서(Overview of the General Data Protection Regulation)('16.7) 발간(ICO 2017a)

– 개인정보처리의 법적 기초, 정보주체의 권리, 개인정보영향평가, 개인정보 유출사고 시 고지의무 등에 대한 구체적 설명 제시

– EU 탈퇴 결정에도 불구하고 GDPR의 중요성 강조(제1장)

○ GDPR 준비를 위해 기관기업이 취해야 할 12가지 조치사항("Preparing for the General Data Protection Regulation 12 steps to take now." ICO 2017b)

– 현행 데이터보호법과 GDPR 간 비교를 통해 체크리스트 제시

표 III-7. 「GDPR 준비를 위해 기관기업이 취해야 할 12가지 조치사항」의 주요내용

① GDPR에 대한 인식(Awareness) • 의사결정자 및 정보처리자가 기존 법률이 GDPR로 대체될 것이라는 사실을 알고 있는지 확인
② 보유하고 있는 정보 파악(Information you hold) • '어떤 개인정보를 보유하고 있는가'를 포함해 해당 정보의 출처 및 정보를 공유하는 상대에 대해 문서로 기록
③ 프라이버시 정보에 대한 커뮤니케이션(Communicating privacy information) • GDPR 시행에 따라 변경이 요구되는 경우 이에 대응하기 계획 수립
④ 개인(정보주체)의 권리 보장(Individuals' rights) • 개인정보 처리 절차에서 정보주체의 권리를 보장하고 있는지 확인
⑤ 정보주체의 데이터 접근 요청 대응 준비(Subject access requests) • 정보주체의 데이터 접근 요청에 대비하여 해당 정보의 출처 및 정보를 공유하는 상대에 대해 문서로 기록
⑥ 개인정보 처리를 위한 법적 근거(Lawful basis for processing personal data) • 현재 수행하고 있는 개인정보 처리의 다양한 유형을 점검하고, 해당 개인정보 처리를 수행하기 위한 법적 근거를 확인하여 문서화
⑦ 동의(Consent) • '동의'는 처리되는 개인정보에 대해 긍정적인 표시를 해야 성립되며, 정보주체가 침묵하거나 체크박스가 미리 채워져 있는 경우 또는 비활성화된 상태를 동의로 유추할 수 없음. • 정보주체의 동의를 바탕으로 개인정보를 처리해야 하는 경우에는 GDPR에서 요구하는 표준을 충족하는지 확인해야 하며, 충족하지 못하는 경우에는 동의 메커니즘을 변경하거나 동의를 대신할 수 있는 방안을 찾을 필요 • 동의는 검증 가능해야 하며, 일반적으로 동의를 바탕으로 개인정보를 처리하는 경우에 정보주체들이 더 강력한 권한을 보유하게 된다는 점에 유의
⑧ 아동(Children)의 개인정보 처리 방안 마련 • 아동 대상의 서비스 제공을 위해 아동의 개인정보를 수집하는 경우, 동의는 입증될 수 있어야 하고, 관련 고지는 아동이 충분히 이해할 수 있는 언어로 작성되어야 함.
⑨ 정보유출(Data breaches) • 개인정보 유출을 탐지·보고·조사할 수 있는 올바른 절차 마련
⑩ 데이터보호 적용설계 및 데이터보호 영향평가(Data Protection by Design and Data Protection Impact Assessments) • ICO의 개인정보영향평가 지침을 숙지하고, 조직에 구현할 방안 준비 • 항상 영향평가를 수행할 필요는 없으며, 새로운 기술 또는 프로파일링 작업이 개인에게 중대한 영향을 줄 수 있는 경우와 같이 위험이 높은 상황에서 필요 • 영향평가 결과 데이터 처리 과정에서 위험성이 높은 것으로 나타난 경우, 해당 처리 작업이 GDPR을 준수하는지 여부에 대해 ICO와 상의하고 의견을 구할 필요
⑪ 데이터보호책임자(Data Protection Officers, DPO) • 정보보호 규정 준수에 대한 적절한 책임을 지고 이를 효과적으로 수행할 수 있는 지식 및 권한을 가지고 있는지 확인
⑫ 국제 이슈(International) • 글로벌 조직의 경우 어떤 국가의 감독기관을 관할로 할 것인지 결정

자료: ICO(2017b).

○ **중소기업 대상 지원**

- GDPR 대응 지원을 위한 전화 서비스('17.11) 등 중소기업이 활용할 수 있는 리소스 패키지 마련
- GDPR 준비 방법에 관한 정보가 필요한 소기업을 대상으로 상기 GDPR 12단계 대응법의 축약 버전 개발
- 중소기업용 툴킷[20]을 GDPR 체크리스트로 개정하여 중소기업들이 GDPR 규정과의 격차를 파악할 수 있도록 지원

○ '디자인 단계부터의 개인정보보호(Data protection by design)'추진('18.3)[21]

- 기업이 제품 출시 전 적절한 개인정보보호 체계를 갖출 수 있도록 **"규제 샌드박스(regulatory sandbox)"를 구축**하여 사전에 테스트할 수 있는 수단 제공
- 제품 생산 초기단계부터 적절한 보안수단을 마련함으로써 이른바 '디자인 단계부터의 개인정보보호' 구현 유도

나. 프랑스

□ 관련 법령 제정 및 기구 권한 확대

○ 프랑스는 GDPR 이행을 위한 첫 단계로서 **2016년 10월 「디지털공화국법」을 제정·공표**

- 프랑스 데이터 보호기관인 CNIL[22]의 권한 및 개인의 권리를 확장하여 개인정보 자기결정권과 통제권 강화

○ CNIL은 개인정보 보호 및 처리와 연관된 모든 법안이나 정부령 혹은 해당

20) 영국 개인정보감독기구(ICO)는 중소기업들이 좀더 상세하게 GDPR을 파악하고, 필요한 규정을 준수하는데 도움을 주기 위해 자가점검 체크리스트, FAQ 등을 묶어 툴킷 형태로 제공하고 있으며, 보다 상세한 정보를 블로그와 웹사이트, 온라인 비디오 등을 통해 안내하고 있다. ICO. GDPR preparation for Small organisations. https://ico.org.uk/for-organisations/business.

21) IT Pro. "UK data watchdog draws up plans for data protection by design."
http://www.itpro.co.uk/general-data-protection-regulation-gdpr/30694/uk-data-watchdog-draws-up-plans-for-data-protection-by

22) 프랑스 국가정보처리자유위원회(CNIL)는 정보처리·축적·자유에 관한 법률(Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) 제6조에 의거해 1978년 독립 행정기관 형태로 창설된 개인정보 규제기관임.

조항들에 대해 의견 제시 가능

○ CNIL 제재위원회(Sanctions Committee)가 부과할 수 있는 벌금 상한액을 대폭 인상한 데 이어, GDPR 시행 이후에는 전세계 매출의 4% 혹은 2천만 유로로 강화할 전망

□ 세부 실행과제 도출 및 가이드라인 개발

○ DPO, 정보이동권, 개인정보영향평가, 인증 등에 대한 공개논의 결과 발표('16.11)

- DPO의 역할과 임무에 대한 명확한 설명이 필요하다는 의견 제기
- 기업은 정보이동권 적용에 따르는 추가 비용과 과도한 경쟁을 우려하면서 대체로 기본의무를 최소한으로 준수하겠다는 입장인 반면, 시민단체들은 이 권리의 광범위한 적용을 지지
- 개인정보영향평가(DPIA)와 관련, 적용 여부를 판단할 명확한 기준과 EU 차원의 일관성 있는 시행을 위한 합의 필요성 제기

○ GDPR 준비를 위한 6단계 방법론(RGDP : se préparer en 6 étapes. '17.3)

- GDPR을 준수하기 위해 필요한 우선순위 업무가이드 제시

표 III-8. 프랑스의 GDPR 준비 6단계 방법론 주요 내용

단계	개요	주요내용
1	DPO 또는 파일럿(Pilot) 임명	• 조직 내에서 데이터 보호 관리를 시범적으로 수행하기 위한 리더 지명
2	데이터 매핑	• 기업조직들이 데이터 처리 활동을 세부적으로 식별할 것을 권장하고, 이를 위해 데이터 처리 활동 등록부를 준비하고 유지
3	GDPR 준수 조치의 우선순위를 지정	• 제2단계에서 등록부를 준비한 후에는 각 데이터 처리 활동에 대해 현재 및 미래의 데이터 보호 의무를 준수하기 위해 구현해야 할 작업을 포착
4	위험 관리	• 제3단계에서 조직이 정보주체의 권리와 자유에 높은 위험을 초래할 수 있는 데이터 처리 활동을 포착한 경우, 이러한 각 데이터 처리 활동에 대해 개인정보영향평가 수행을 권고
5	내부 프로세스 구성	• 데이터 처리의 생애주기 동안 발생할 수 있는 모든 사건을 고려하여 언제든지 데이터 보호를 보장하기 위한 내부 절차 구현 권장
6	규정 준수 조치에 관한 문서 보관	• 동 절차의 마지막 단계에서 조직은 필요한 모든 문서를 함께 컴파일하고 그룹화하며, 지속적인 데이터 보호를 위해 각 단계에서 생성된 작업 및 문서를 정기적으로 재검토하고 업데이트

자료: CNIL. RGPD : se preparer en 6 etapes
https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes.

○ GDPR 준수를 위한 가이드라인(GUIDE DU SOUS-TRAITANT) 제시('17.9)

– ▲ 데이터 처리와 관련된 체크리스트, ▲ 데이터처리 업무를 보조할 서브-프로세서 지명, ▲ 개인정보영향평가 수행 지원, ▲ 데이터 유출 고지 등과 관련한 데이터 처리자의 의무 설명

– 데이터 프로세서가 숙지해야 할 제재시스템 소개, 제재를 유발할 수 있는 위반 사례 제시

○ 온라인 공개 자문('17.9.19~10.19)

– 규정 해석, 데이터 처리의 투명성과 국경 간 데이터 전송 등에 대한 질의 답변, 모범사례 제시

○ 개인정보 영향평가를 위한 소프트웨어 개발('17.11)[23)]

– 데이터 컨트롤러가 개인정보 영향평가를 수행하는데 도움을 줄 수 있는 오픈소스 기반의 소프트웨어 개발

– 개인정보 처리의 유형·목적·배경, 정보주체의 권리 등 기본 원칙에 대한 컴플라이언스 정보, 잠재적인 프라이버시 위험과 이를 감소시키는 방안 등을 시각적으로 제시

다. 독일

□ 관련 법령 제정

○ 독일은 EU 회원국 최초로 2017년 7월 GDPR에 부합하는 독일 연방 데이터 보호법(Federal Data Protection Act; Bundesdatenschutzgesetz, BDSG)[24)] 제정('17.7.5)하여 2018년 5월 25일 발효 예정

– 독일 연방의회는 2017년 4월 새로운 독일 연방 데이터보호법(BDSG) 법안을 승인하였으며, 이 법안은 독일 연방 상원의 검토과정을 거쳐 2017년 7월

23) IAPP. CNIL releases PIA software for the GDPR:Here's how it works. https://iapp.org/news/a/cnil-releases-pia-software-for-the-gdpr-heres-how-it-works/

24) 독일개인정보보호개정법(GDPAA, German Data Protection Amendment Act)으로도 불림.

입법과정의 최종단계를 통과

□ GDPR 준수를 위한 가이드라인 개발

○ 독일 바이에른 주(州) 데이터보호국은 GDPR 제재조항, 데이터 국외이전, 원스톱숍 등 주요 이슈에 대한 가이드를 발표

– GDPR 규제 준수를 위해 실질적으로 필요한 조항에 대한 해석 제시

표 Ⅲ-9. 독일 바이에른 주(州) 데이터보호국(DPA)의 주제별 가이드라인 개요

발표시기	제목	주요내용
'16.09	GDPR 제재 조항	• GDPR 제제 조항의 세부내용
'16.11	데이터 국외이전	• 타국으로의 데이터 전송 관련 사항에는 대부분 현재의 법이 적용되어 있으며, 행동 강령(Codes of Conduct)과 인증(Certification) 등의 내용이 포함된 새로운 법규정으로 보다 유연성 있는 데이터 보호 시스템 구축
'16.12	원스톱숍	• 원스톱숍(OSS) 개념을 도입하며 하나의 기관이 담당한 곳의 개인정보처리 업무를 일괄적으로 감독 • 국경을 넘는 정보의 처리 과정에서 실질적인 행정적 간소화와 기업에 대한 더 많은 법적 보호 기대
'17.03	개인정보영향평가	• 규정된 방법으로 위험을 분석하며 개인정보영향평가를 수행하고 위험 요소들은 적절한 대책으로 감소시킴(감독기관은 수행 활동을 보고, 발표할 의무) • 바이에른주 DPA는 개인정보영향평가 주요 수단에 대한 내용 등을 실제 예시와 함께 웹사이트에 게재
'17.05	데이터 보호 담당 기관	• 데이터 보호 담당 기관을 정하는 기준과 기관의 과제, 책임, 업무, 위법 시 법적 절차 등 규정 (37~39조) • 29조 작업반은 이에 대해 자세히 설명하고 있고 이는 보고서로 작성되어 인터넷 열람 가능
'17.05	광고를 위한 개인정보 처리	• GDPR 제6조에 의거하여 적용 • 필요시 EU 가이드라인 고려

자료: Bavarian Data Protection Agency(BayLDA). EU General Data Protection Regulation. https://www.lda.bayern.de/en/privacy_eu.html

라. 기타 국가

□ **(벨기에)** GDPR 준수를 위한 13단계 로드맵(PRÉPAREZ-VOUS EN 13 ÉTAPES. '17.5) 발표

– GDPR에 대한 인식 제고와 업계와의 명확한 협약을 체결하는 것이 최우선

과제임을 확인, 개인정보 침해 문제와 관련한 조정자 역할의 중요성 강조

- 과징금은 GDPR 준수를 공식적으로 거부하는 경우 등에 대한 최후의 수단으로만 부과할 것임을 강조

표 III-10. 벨기에의 GDPR 준수 13단계 로드맵

단계	제목	주요내용
1	인식	GDPR 체제로의 이행을 위한 핵심 인물과 의사결정자 확인
2	데이터 등록	현재 보유중인 개인정보와 그 출처 등의 인벤토리 작성
3	커뮤니케이션	기존 개인정보취급 방침이나 개인정보보호 계획이 GDPR에 맞춰 변경되어야 할 것인지 여부 확인
4	데이터 처리권한 검토	개인정보데이터의 삭제 권한 등 조직 내에서 개인정보를 취급할 수 있는 담당자의 권한 검토
5	데이터 접근권한 검토	GDPR에 따라 데이터 접근을 위한 요구사항을 어떻게 충족할 것인지 점검
6	데이터 처리의 법률적 기반 확인	현재 수행 중인 다양한 유형의 데이터 처리 현황에 대해 문서를 작성하고 각각의 경우에 대한 법률적 근거 확인
7	동의 문제	정보주체의 동의를 구하고 정보를 획득・등록하는 방식에 대해 검토,필요한 경우 변경 추진
8	아동의 개인정보	데이터주체의 연령을 확인할 수 있는 시스템을 개발하고, 데이터 처리를 위해 부모나 후견인의 동의를 구하는 절차 정비
9	데이터 유출	개인정보의 유출에 관한 탐지・보고・분석을 위한 적절한 절차 확보
10	프라이버시 중심 설계/개인정보영향평가	프라이버시중심설계와 개인정보영향평가(PIA)에 대한 개념과 원칙에 익숙해지고, 이 두 가지를 비즈니스 과정이나 조직 내에서 구현하기 위한 방안 모색
11	DPO	필요한 경우 DPO를 지명하고, 조직 내에서 DPO의 위상 검토
12	글로벌 이슈	글로벌 활동 기업의 경우 국경간 데이터 처리와 관련한 책임자 결정
13	기존계약 검토	데이터 위탁처리 등과 관련한 기존 계약을 검토하고, 필요한 경우 적절한 시기 내에 계약 내용 변경

자료: CPVP(Commission for the Protection of Privacy, Belgium). PRÉPAREZ-VOUS EN 13 ÉTAPES. https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

○ 벨기에 개인정보감독기구는 DPO 임명 시 필요한 권장내용 발표('17.6)

- DPO의 역할과 임무를 설명, DPO를 임명하는 회사에 대한 요구사항과 DPO가 목표를 수행하기 위해 갖춰야 할 자격요건 열거

- 현재 벨기에의 정보보호 체계 하에서 지정된 보안 책임자(security officers)는 GDPR 하에서의 DPO로 자동 지정될 수 없음을 명시

□ **(스위스)** EU 회원국은 아니지만 GDPR에 대응하여 데이터보호법 개정 진행

○ GDPR에 부합하는 새로운 데이터보호 법안의 예비초안(Draft-DPA) 준비[25)]

– 스위스 정부는 2017년 4월 4일까지의 공개의견 수렴기간 중 논의된 협의결과를 검토하고 이를 반영한 최종초안을 의회에 제출

○ 스위스 연방 위원회(Swiss Federal Council)는 2017년 9월 15일 스위스 연방 데이터 보호법 개정을 위해 상기 초안 채택

– GDPR과는 달리 ▲ 데이터 이동성에 대한 권리를 인정하지 않고, ▲ 국외(extra-territory)의 범위를 제시하지 않으며, ▲ 동의와 인증 메커니즘에 대한 요구사항이 덜 엄격하고, ▲ 과징금 등 제재가 제한적

□ **(EU 역외 영미권 국가)** EU와의 무역을 위해 GDPR 대응체계 수립 중

○ 미국은 EU와의 Privacy Shield 협정을 통해 대응하고 있으므로 정부차원의 적극적인 움직임은 없지만, 글로벌 기업을 중심으로 GDPR 준비[26)]

○ 캐나다는 EU 적합성 인정을 유지하기 위해 개인정보보호법(Personal Information Protection and Electronic Documents Act, PIPEDA)을 GDPR에 부합하도록 개정 중

○ 호주는 정보위원회(OAIC)는 EU와 교역하는 기업들을 위한 가이드라인을 제시, 자국 개인정보보호법과 GDPR의 주요 차이점 등 공개

25) Lexology. 2017. "Switzerland to Overhaul its Data Protection Framework." https://www.lexology.com/library/detail.aspx?g=fe5bd158-c73c-4721-bb28-7ff4c604855a

26) GDPR 준수를 지원하기 위한 상업적 목적의 솔루션 개발 및 출시 등이 이루어지고 있음.

4 한국 정부의 대응

□ EU 개인정보보호 적정성 평가 추진

○ 한국정부는 국내기업이 EU 규제당국의 별도 규제심사를 거치지 않고 개인정보 이전할 수 있도록 정보통신망법 기반의 적정성 평가[27] 승인 추진 중

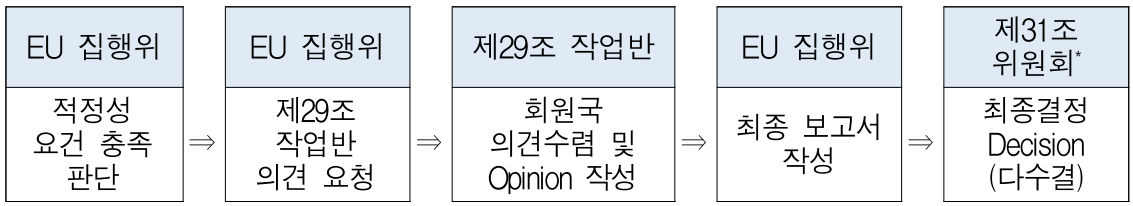
– 적정성 평가(adequacy decision)는 제3국이 EU가 요구하는 수준으로 개인정보 보호조치를 갖추고 있는지 평가하는 제도

○ **적정성 평가를 받을 경우, EU 회원국별로 상이한 개인정보 보호규제의 준수를 위한 비용과 사업지연 등 문제를 방지**할 수 있음.

– 적정성 평가를 받지 않은 국가의 기업은 사전에 개인정보 역외이전 계약 체결 후 EU 회원국 감독기구(DPA)의 심사를 받아야 개인정보의 국내 전송·처리가 가능

○ 단, 이는 국외이전과 관련된 사항이며 GDPR의 규정을 준수해야 한다는 의무에는 변함이 없음.

그림 III-1. EU 적정성 평가 단계 및 주체



*: EU 개인정보보호지침 제31조에 의해 설치된 위원회로 적정성평가 심사
자료: 한국인터넷진흥원.

27) 적정성 평가 기준은 목적제한, 정보의 정확성 및 비례성, 투명성, 안전성, 열람 정정 및 이의 신청의 권리, 재이전 제한 등의 6개 기본원칙과 민감정보 처리제한, 직접 마케팅 제한, 개인에 대한 자동화된 의사결정 제한 등 3개 추가원칙 등을 포괄하는 내용적 판단기준을 적용함. 또한 보호원칙 준수체계 확보, 정보주체 권리행사 지원 및 보호체계, 적절한 구제조치 등의 절차적 판단기준을 통해 평가함. 더불어 국가기관에 의한 개인정보 접근 및 활용(public authority's access) 제한 등 평가 기준을 강화함. 2018년 3월 1일 현재 적정성 승인을 받은 국가는 스위스(00.7월), 캐나다 (01.12월), 아르헨티나(03.6월), 건지 섬(03.11월), 맨 섬('04.4월), 저지 섬(08.3월), 페로 제도(10.3월), 안도라(10.10월), 이스라엘(11.1월), 우루과이(12.8월), 뉴질랜드(12.12월), 미국(16.7월)으로 총 12개국임.

○ 추진 경과

– 정보통신망법 중심의 자체평가 보고서 개발 및 EC 대면 회의(‘17.6)

– 방통위는 유럽평의회 개인정보보호조약(CoE 108호)에 옵저버 가입(‘17.6)

– 자체평가 수정보고서 제출(‘17.9) 및 관련 질의 수시 대응

– 한-EU 고위급 회담 및 공동성명서 발표를 통해 양국 간 협력 강화 및 조속한 시일 내 적정성 평가승인 합의(‘17.11)

– EC 적정성 평가 담당책임자와의 정기적인 대면 및 화상회의 개최를 통해 상호 개인정보보호 법제 환경에 대한 이해 제고

○ **적정성 평가 승인에 따른 기대 효과**

– 기업이 개별적으로 체결해야 하는 역외이전 계약, 해당국가 감독기구 규제심사 비용 절감 등 국내 기업의 EU 진출 여건 개선

– EU 법제에 대한 인지도가 낮고, 개별 계약체결 비용을 부담하기 어려운 정보통신망법 적용 대상 중소·스타트업 기업 등 수혜 예상

□ 기업을 위한 GDPR 안내서·가이드 발간 및 세미나·간담회 개최 등

○ GDPR에 대한 인식제고와 대응력 제고를 위해 안내서(’17.5), 제1차 가이드(’17.12) 발간, 2차 최종 가이드(가칭 가이드북) 발간 예정

– 기업이 반드시 알아야 할 주요 조치사항을 안내하고, 기업 스스로 GDPR 준수 역량을 진단할 수 있는 자가 점검 기준 제시

– EU 29조 작업반이 발표한 가이드라인과 주요 각국의 대응사례를 종합하여 국내 기업 실정에 맞는 최종 가이드북 발간 예정

○ GDPR 대응수준 제고를 위한 세미나, 간담회 등 개최

– 기업을 대상으로 한국인터넷진흥원, 코트라 등 유관기관이 한국과 EU 현지 세미나를 개최하여 실제 적용 및 모범사례 발굴, 전파 추진 중

표 III-11. EU의 29조 작업반 가이드라인 발간 현황

번호	제목	발표 시기
1	· DPO 임명 (Data Protection Officer)	2017.4.
2	· 개인정보 이동권 (The right to data portability)	
3	· 선임 감독기구 (The lead supervisory authority)	
4	· 개인정보 영향평가 및 고위험 초래 개인정보처리(Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk”)	2017.10.
5	· 과징금 부과 (The application and setting of administrative fines)	
6	· 자동화된 의사 결정 및 프로파일링(Automated decision-making and profiling)	2017.10.
7	· 개인정보 유출 통지 (Data breach notification)	
8	· 동의 (Consent)	2018.1.
9	· 투명성 (Transparency)	2018.1.
10	· 국외이전 (Data transfers to third countries)	2018.2.
11	· 인증 기구(Certification Bodies)	2018.2.

주: 적정성 평가 참고 자료(Adequacy Referential), 구속력 있는 기업 규칙(Binding Corporate Rules, BCR), 프로세서용 구속력 있는 기업 규칙(Processor Binding Corporate Rules) 등 발표

자료: European Commission. Article 29 Newsroom. http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

5 기업의 준비과제[28]

가. GDPR 인식 제고 및 준비를 위한 조치사항

□ GDPR 준수를 위한 인식제고

- ○ 조직의 의사결정에 관여하는 관리자들의 적극적인 참여 유도
- ○ GDPR의 주요 내용을 확인하고, 이를 조직에 알리는 등 적극적인 인식제고 활동 수행
- ○ GDPR의 개인정보 처리방식과 조직의 처리방식의 차이 분석
- ○ DPO를 선임하고 GDPR 규제조항 준수를 위한 이행계획 수립
- ○ 조직의 책임성 이행사항을 입증할 수 있도록 적절한 문서화 수행

□ GDPR의 적용범위 확인

- ○ 물적, 지역적, 인적 적용범위 및 적용예외 여부 확인

그림 III-2. GDPR의 적용 범위

자료: 행정안전부·한국인터넷진흥원(2017b).

28) 본 절의 자세한 내용은 행정안전부·한국인터넷진흥원. 2017b.「우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 1차 가이드라인」참고.

□ GDPR의 준수 검토 및 모니터링

○ 조직이 보유하고 있는 개인정보의 유형과 처리방식, 규모 파악

○ 개인정보의 목록 및 흐름을 파악하여 적절한 모니터링과 통제가 이루어질 수 있도록 조치

○ GDPR 전반의 요구사항에 부응할 수 있는 자체 대응체계 마련

나. 책임성 강화를 위한 조치사항

□ 개인정보 보호 적용설계(Data Protection by Design and Default)

○ 조직 내 IT 개발절차를 확인하고, 어플리케이션·제품·서비스의 기본 설정이 개인정보 보호를 위해 친화적인지 검토하여 부족한 부분에 대한 보완을 실시

♣ 개인정보 보호 적용설계의 7대 기본원칙 ♣

Proactive not reactive – preventative not remedial	선제적-사후조치 및 보완이 아닌 사전 예방
Lead with privacy as the default setting	프라이버시 보호가 가능하도록 기본설정
Embed privacy into design	설계 자체에 프라이버시 내재화
Retain full functionality (positive-sum, not zero-sum)	충분한 기능성 유지(포지티브섬)
Ensure end-to-end security	종단간 보안 확보
Maintain visibility and transparency – keep it open	가시성과 투명성 유지
Respect user privacy – keep it user centric	이용자 프라이버시 존중 - 이용자 중심

♣ 개인정보 보호 적용설계의 구체적인 적용방안 ♣

◆ 개인정보 영향평가(PIA, Privacy Impact Assessment) 수행

- 개인정보를 활용하는 새로운 정보시스템의 도입 및 기존 정보시스템의 중요한 변경 시, 시스템의 구축과 운영이 정보주체에게 미칠 영향에 대해 조사·분석·평가하는 체계적 절차

◆ 프라이버시 중심의 기본 설정 제공

- 정보주체(이용자)에게 제공되는 서비스의 기본 설정(default settings)이 프라이버시가 충분히 고려된 방식인지 검토

◆ 프라이버시 보호기술(PETs, Privacy-Enhancing Technologies)의 적용

- 프라이버시 보호기술은 정보통신 시스템의 기능을 저하시키지 않고, 개인정보를 제거 혹은

최소화함으로써 불필요하거나 원치 않는 개인정보의 처리를 예방하여 정보 프라이버시를 보호하는 방식

◆ "적절한 수준의" 기술적·관리적 조치의 적용

- GDPR은 적절한 기술적, 관리적(조직적) 조치 적용시 다음 사항을 고려(Article 25(2))

"적절한 수준"의 기술적·관리적 조치 적용시 고려사항	
수집한 개인정보의 양(amount)	개인정보 처리의 범위(extent)
저장 기간(period)	접근 가능성(accessibility)

자료: 한국인터넷진흥원(2018).

□ DPO 임명

○ 개인정보 처리를 위해 의무적으로 DPO를 임명해야 하는지 파악

○ DPO 임명 시, 전문적 자질, 개인정보보호 법령에 대한 지식, 감독 기관과의 협업 경험, 관계자와의 커뮤니케이션 능력 고려

○ DPO의 업무 독립성을 보장하고 이해 충돌을 방지

□ 개인정보 영향평가(DPIA) 시행

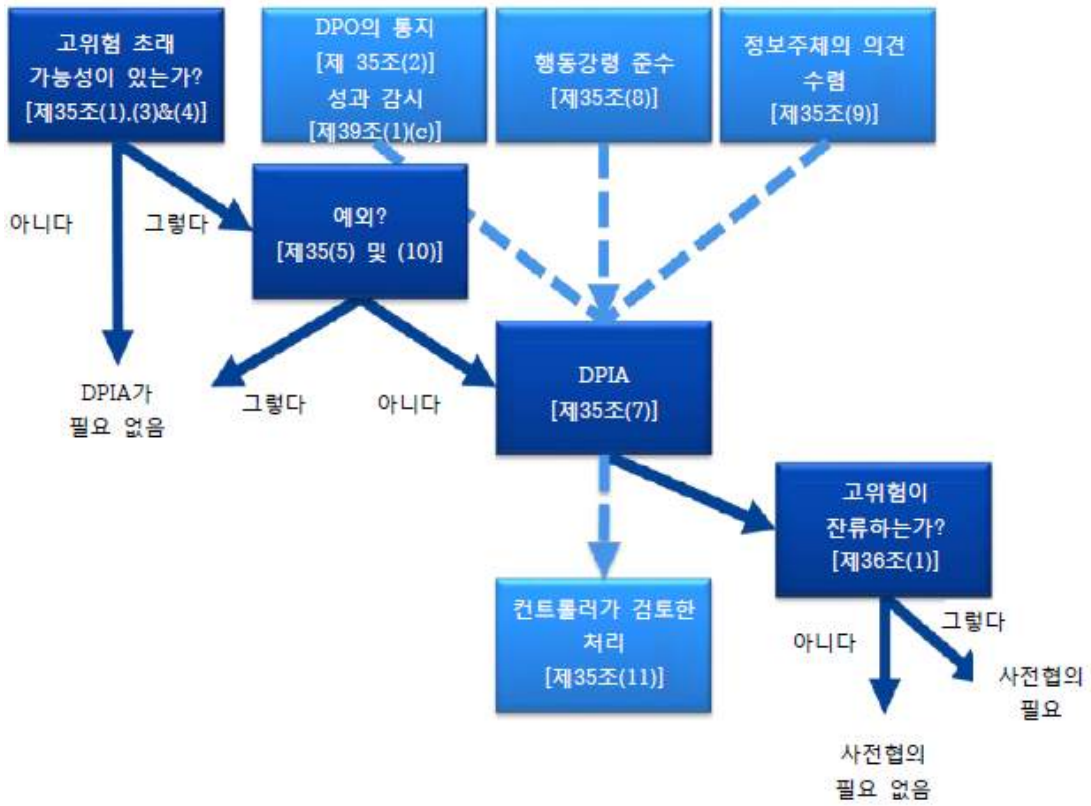
○ 개인정보 영향평가를 의무적으로 수행해야 하는 경우에 대해 파악

○ 개인정보 영향평가 실시 요건과 방법 파악

○ 개인정보 처리가 이루어지기 전에 개인정보 영향평가 수행

○ 감독기구와 협의가 필요한 경우에 대해 파악

그림 III-3. GDPR의 개인정보영향평가 수행단계 흐름도



자료: 행정안전부·한국인터넷진흥원(2017b).

□ 개인정보 국외이전 시 필요사항

○ 조직에서 처리되는 개인정보를 식별하고 국외 이전되는지 확인

○ 국외이전에 적합한 매커니즘(표준계약, 구속력 있는 기업규칙(BCR), 행동강령 및 인증제도 등) 파악

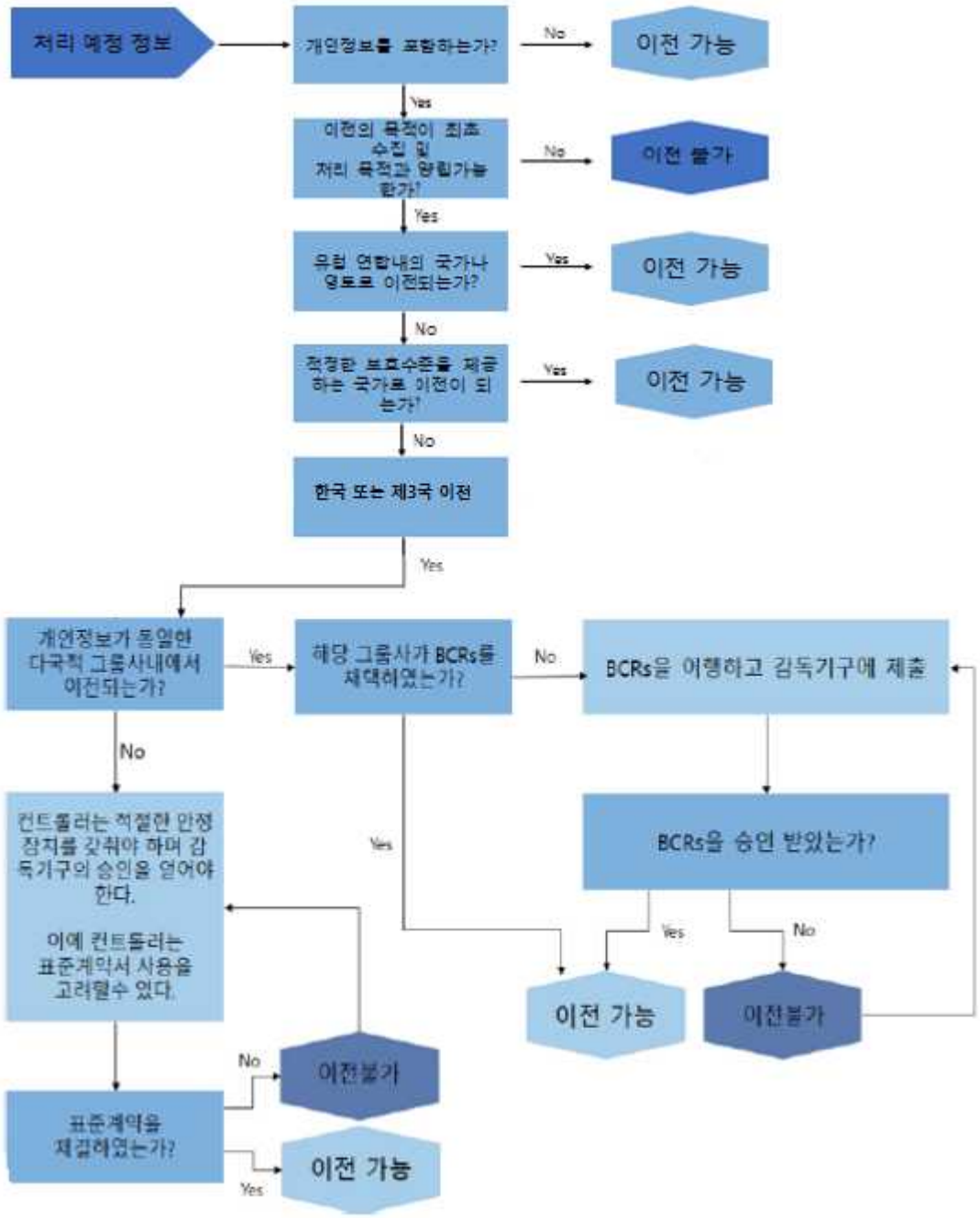
○ 조직의 개인정보의 이전이 국외이전의 특정한 예외상황(명시적 동의, 계약 이행, 공익상의 이유 등)에 해당하는 지 확인

□ 선임 감독기구 파악

○ 개인정보를 "국외처리(Cross-border processing)"하는지 확인

○ 선임 감독기구(lead supervisory authority)와 유관 감독기구(concerned supervisory authority) 파악

그림 Ⅲ-4. 기업의 GDPR에 의한 개인정보 국외이전 체제 예시



자료: 행정안전부·한국인터넷진흥원(2017b). MyData-Trust(2017)에서 인용한 도표 일부 수정.

다. 정보주체의 권리 강화를 위한 조치사항

□ 삭제권(잊힐 권리, right to erasure 또는 right to be forgotten) 보장

○ 삭제권과 관련된 내부 지침 및 절차를 마련하고 처리되는 개인정보의 식별 및

그 흐름을 파악

○ 삭제권을 보장하기 위한 체계를 수립하여 이행

□ **개인정보 이동권(Right to data portability) 보장**

○ 정보주체로부터 개인정보 수집 시 개인정보 이동권 고지 절차 마련

○ 정보주체로부터 정보 이전을 신청 받은 경우, 개인정보 이동권의 범위에 포함되는지 확인

○ 정보주체의 정보 이전 신청 처리 절차 및 기계로 판독이 가능한 개인정보 이전 방법 마련

□ **자동화된 결정 및 프로파일링 관련 권리 보장**

○ 조직 내 프로파일링 현황을 파악하고 프로파일링이 개인정보의 자동화 처리를 기반으로 개인의 특성 평가를 위해 이루어지는지 확인

○ 프로파일링을 기반으로 자동화된 의사결정이 이루어지는지 확인

○ 자동화된 의사결정이 유발하는 효과 확인

○ 프로파일링 기반 자동화된 의사결정을 활용하는 업무의 수행 근거 확인

○ 정보주체의 권리(정보를 제공받을 권리, 열람권, 완전히 자동화된 의사 결정의 대상이 되지 않을 권리 등) 보장 절차를 마련

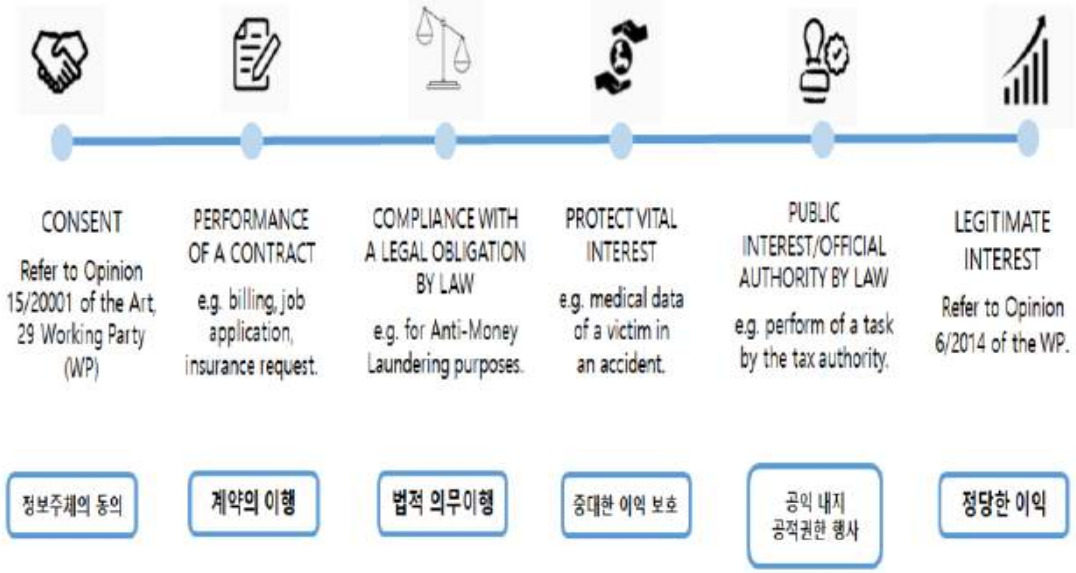
○ 민감 정보와 아동의 개인정보가 처리되는지 확인

○ 자동화된 결정 및 프로파일링 관련 권리 보장을 위한 보호조치(safeguards) 마련

○ 자동화된 의사 결정을 개인정보 영향평가(DPIA) 대상에 포함

○ 프로파일링에 GDPR 개인정보보호 원칙의 적용 여부 확인

그림 III-5. GDPR에서의 개인정보 처리 적법성 요건



자료: 행정안전부·한국인터넷진흥원(2017b).

Ⅳ 결론

1 GDPR의 평가와 전망

□ GDPR은 EU 특유의 여건에서 경제·공익적 가치의 조화를 추구한 결과물

○ 유럽은 전통적으로 프라이버시를 인권으로 간주, EU 시민은 프라이버시에 대한 민감도가 매우 높음.

– 유럽 시민 10명 중 8명이 개인정보를 스스로 완전히 통제하지 못한다고 인식(European Commission 2015)

– 개인정보의 역외 이전에 대한 신뢰성 있는 체제를 구축함으로써 역외로 나간 개인정보의 유출에 대한 우려 해소

○ EU는 역내 개인정보보호법을 조화시키고 데이터 이동을 효율화함으로써 거대시장을 기반으로 한 디지털 혁신 추진

– 온라인상으로 수집되는 개인정보의 보호와 활용이 점차 국제무역 및 기업 활동의 일상적인 활동이 됨에 따라, EU는 정보의 효율적이고 안전한 활용을 보장할 수 있는 제도 구축에 노력

– 개인정보 보호 적용설계(data protection by design) 원칙을[29] 도입하여 역내기업의 개인정보 보호역량을 강화하고 데이터기반 혁신을 촉진

– 회원국간 개인정보보호법의 차이를 완화함으로써 역내 기업의 행정비용 절감 규모는 연간 23억 달러에 달할 것으로 추정[30]

□ (기업활동에 대한 영향) GDPR은 단기적으로 개인정보 보호에 대한 비용부담을 증가시키고, 개인정보 기반 혁신을 제약할 가능성을 안고 있음.

○ 역내 중견·중소기업의 GDPR 적응비용은 연간 3,000~7,200 유로로 추산되

29) 자세한 사항은 다음 절 참고.
30) European Commission(2012).

며(Christensen et al. 2013), EU 개인정보 체제에 익숙하지 않은 역외 기업의 적응비용은 더 클 것으로 예상

○ 개인정보 활용 제약에 따른 기업의 비즈니스 혁신 제약으로 인해 경제성장과 고용에 대한 부정적 영향 가능성 제기(ECIPE. 2013; Deloitte, 2013 등)

□ **(무역에 대한 영향) GDPR이 무역장벽으로 작용하여 EU로의 서비스 수출이 감소하는 효과가 나타날 것이라는 전망 제기**

○ EU 역내 기업이 서비스 조달처를 역내 기업으로 전환함으로써 미국의 對EU 서비스 수출은 16.4%에서 최대 23.8% 감소할 것이라는 전망 제기

– 역외기업들은 GDPR의 비용요인 및 구체적인 적용내용의 불확실성으로 인해 수출 대신 EU 역내 투자로 전환할 가능성 → EU로의 수출 감소

– 더욱이 EU의 서비스 수입 감소는 역내 기업의 경쟁력을 떨어뜨려 결국 EU의 수출 역시 감소시킬 가능성(이상 ECIPE 2013)

○ 유럽 기업들이 데이터 분석 업무를 인하우스로 전환할 가능성

– 개인정보 분석을 외주로 돌릴 경우 예상되는 리스크를 회피하기 위해 이를 사내에서 수행하겠다는 기업이 증가할 수 있어, 외주 기업에 불리하게 작용할 것이라는 예상(London Economics 2017)

○ 단, GDPR은 데이터의 국경간 이동에 다양한 방식을 두고 있는바, 장점으로 평가됨.

– 소비자 개인의 동의(Consent) 일변도에서 탈피, BCR, 표준계약 등 다양한 방식을 활용한 개인정보 국외 이전이 가능

□ **(한국의 수출·투자에 대한 영향)** 對EU 수출·투자의 특성상 GDPR은 중요한 제도적 변화가 될 전망[31]

○ 한국의 對EU 수출은 데이터 혁신 및 플랫폼 비즈니스와 직간접적으로 연

31) 자세한 사항은 제2장 참고.

계된 전자·전기, 기계류, 소비재·식품류 중심으로 호조

- 서비스 수출의 경우, 최근 對EU 지식재산권사용료, 통신·컴퓨터·정보서비스, 기타서비스 분야의 수출이 증가

○ 투자의 경우, GDPR과 직결될 수 있는 전문·과학·기술 서비스업, 출판·영상·정보통신 서비스업 투자가 큰 비중을 차지

- 전문·과학·기술 서비스업 가운데서는 전문서비스업 투자가 주종을 이루며, 출판·영상·정보통신 서비스업에서는 통신업, 출판업, 정보서비스업이 큰 비중

○ 한국 스타트업은 데이터 집중도가 높은 분야를 중심으로 유럽 진출

- 한국 스타트업의 유럽 진출 비중은 8.1%로 상대적으로 낮지만,* 개인정보 활용 빈도가 높은 전문·과학·기술 서비스, 출판·영상·정보통신 서비스, 교육서비스업 등 고부가 영역에 집중

* 해외 진출 창업기업 가운데 68.3%가 동북아, 29.0%가 동남아시아에 진출하고 있으며, 북미 진출 기업은 10.3%(창업진흥원 2017)

□ **(전망)** 경제적 측면의 우려에도 불구하고, 온라인 개인정보 보호에 대한 관심이 높아지는 여건에서 **GDPR과 유사한 내용의 개인정보보호법과 국경간 개인정보 이전 규정이 확산될 가능성이 높음.**

○ GDPR은 데이터 수집, 이용, 저장 등에 대한 새로운 권한을 부여하여 정보주체의 권한을 대폭 강화한다는 점에서 의의가 있지만, 유럽연합 이외의 국가들에게는 거부할 수 없는 선택을 강요하는 측면도 있음.

- 과거 유럽의 제국주의 권력이 현대의 글로벌 디지털경제에서 재현되는 상황으로 평가되기도 함(Scott and Cerulus 2018).

- EU와는 상이한 개인정보 보호법제를 운영 중인 미국은 EU와 정부간 Privacy Shield 협정을 체결하여 자국 기업이 EU가 요구하는 수준의 개인정보 보호를 이행토록 하고 있음.

- 우리나라와 일본은 EU의 개인정보보호 적정성 평가 심사를 추진하면서 EU와의 개인정보보호법 호환성을 높이는 과정에 있음.

– 유럽 이외 국가 가운데, 한국, 일본, 호주, 말레이시아, 싱가포르, 러시아, 캐나다, 멕시코 등이 EU와 유사한 개인정보 보호법 운영*

* BSA의 조사에 따르면 조사 대상 24개국 가운데 17개국이 EU와 유사한 형태의 개인정보 보호법제를 운영 중(2017년 현재. 다음 표 참고)

○ ① 데이터 혁신을 주도하는 미국과 중국에 대한 견제 심리와, ② 개인정보를 활용한 혁신 필요성, 그리고 ③ 개인정보 유출에 대한 우려가 맞물려 GDPR은 세계 각국법의 주요한 벤치마크가 될 가능성이 높음.

○ 요컨대, 디지털 혁신 시대와 맞물려 **EU는 GDPR을 통해 자국의 개인정보 보호법을 '수출'하는 효과를 거둘 것으로 전망**됨.

표 Ⅳ-1. 주요국의 개인정보 보호법

국가	프라이버시법 유무	프라이버시법 범위	EU 개인정보 보호법과의 상응성	APEC 프라이버시 프레임워크와의 호환성
아르헨티나	O	포괄법	O	X
호주	O	포괄법	O	O
브라질	추진 중	-	-	-
캐나다	O	포괄법	O	O
중국	부분적	분야별	-	-
프랑스	O	포괄법	O	O
독일	O	포괄법	O	O
인도	부분적	분야별	-	-
인도네시아	부분적	포괄법	-	-
이탈리아	O	포괄법	O	O
일본	O	포괄법	O	O
한국	O	포괄법	O	O
말레이시아	O	분야별	O	O
멕시코	O	포괄법	O	O
폴란드	O	포괄법	O	X
러시아	O	포괄법	O	O
싱가포르	O	포괄법	O	O
남아공	O	포괄법	O	X
스페인	O	포괄법	O	X
태국	추진 중	-	-	-
터키	O	포괄법	O	X
영국	O	포괄법	O	O
미국	부분적	분야별	X	O
베트남	부분적	분야별	-	-

주: 위의 표는 24개 국가에 대한 조사결과 전체임.
자료: BSA(2018).

2 대응방안

가. 개인정보 보호 패러다임의 변화

□ 개인정보는 가치창출의 핵심 자원

○ 4차산업혁명의 궁극적 지향점은 데이터 분석을 통해 맞춤형 제품·서비스를 공급하는 것으로서, 개인정보의 수집·분석이 핵심

– 과거의 거래나 무역이 B2B 중심이었다면, **앞으로는 데이터 혁신을 통해 B2C 접점이 늘어날 전망**

○ 수집되는 데이터의 종류와 양이 증가하고 이를 분석하는 기술 역시 발전함으로써 몇 가지 데이터를 조합하여 개인을 식별하는 것이 가능해짐에 따라, **개인정보의 범위가 넓어지는 추세**

– GDPR에서 확인할 수 있듯이 자연인을 직접 또는 간접적으로 식별 가능한 경우라면, 성명·주소 등과 같은 일반적인 개인정보 외에 온라인 식별자나 위치정보도 개인정보에 해당될 수 있음.

□ 인터넷을 통해 대규모 데이터가 전송 가능해지면서 **국경을 초월한 데이터의 전송과 수집이 일반화**(아래 표 참고)

○ 사물인터넷을 통해 연결된 기기나 어플리케이션을 통해 국경을 넘어 실시간으로 대량 정보가 수집되는 현상이 일반화*

* 앱을 통한 거래한 내역이나 행태정보, 검색엔진에서의 활동내역 등이 국외 데이터센터에 저장되거나 소재국을 파악하기 어려운 클라우드에 저장되는 것이 일반화

○ 미국이 국경간 데이터 이동의 자유화를 통상협상에서 강력하게 주장하는 것이나, EU가 디지털단일시장전략의 핵심적인 과제로 GDPR을 비롯한 국경간 데이터 이전 관련 제도를 정비하는 것 모두 미래 산업경쟁력 확보 차원에서 중요한 의미

표 IV-2. 기업의 비즈니스 활동 중 발생하는 국경간 데이터 이동 사례

유형	내용
기계간 연결	생산라인의 상호연결을 통한 생산공정 개선 및 효율성 최적화 - 실시간 생산장비 모니터링을 통한 정지시간 절감, 즉각적인 서비스 대체 등
빅데이터 분석	각 지역의 모든 운영 프로세스에서 발생하는 데이터 수집 , 이를 분석하여 사업 개선 및 소비자 만족 증대를 위한 의사결정에 적용
업무 개선 ·통합	각 지역에 중복 ·산재된 기능의 통합 및 효율화 - 예 : 분산된 구매, 회계, 급여 시스템, HR 콜센터 등의 통합 - 예 : 유니레버 , 텐센트 , IBM 등 글로벌 기업의 HR 시스템 통합
공급사슬 자동화	재고 추적 관리 , 재주문 절차 자동화 , 수요공급 매칭 등
디지털 협업	모바일기기 , 클라우드서비스를 활용하여 팀간 소통 및 협업 활성화 - 예 : 보이스 ·웹 ·화상회의 , 정보 공유 , 공동 작업
클라우드 사용	IT 하드웨어, 인프라, 소프트웨어 등 자본 지출 절감, 사업유연성 확보
IT 기반 제품 개선과 서비스 제공	IT 를 활용한 제품과 서비스의 글로벌 공급 - 예: 소셜미디어, 모바일앱, 크라우드소싱 등을 적용한 비즈니스 확산 - 예 : 거점 지역에 IT 기반 헬프 데스크 구축 - 예 : 신용카드회사의 글로벌 네트워크

자료: Business Roundtable(2015).

□ 개인정보 보호와 활용 사이의 균형을 찾는 것이 기업과 정부의 과제

○ 현재의 개인정보 보호는 기업 이익과 공익적 관점 사이의 균형을 요하는 사안으로서, **비용요인으로만 이해하기는 어려운 상황**

○ 사물인터넷 등 개인정보 수집 기술과 채널이 급격히 발전하면서 개인정보 침해 우려가 급증하는 반면, 개인정보 활용을 활성화할 필요성도 대두

– 예컨대 사물인터넷 기기의 연결 증가로 데이터량이 폭증할 것으로 예상되면서 취약점을 노린 개인정보 침탈행위에 대한 우려 증대

– 반면 개인정보의 활용을 활성화한다는 취지에서는, 불필요한 제도적 걸림돌을 제거하는 것이 각국정부의 주요 과제로 대두

○ 이러한 배경 하에서 프라이버시 보호 관점과 더불어 기업활동 및 경제·산업정책과 맞물려 국내외 개인정보 체제에 대한 논의가 활발하게 진행

– 데이터의 국경간 이동 자유화 수준 제고, 국가간 개인정보 보호체제의 호환성을 향상시키는 문제는 통상협상 등 글로벌포럼의 쟁점으로 등장

나. 기업의 대응방안

□ GDPR을 EU와의 교역을 위해서 뿐만 아니라, 전반적인 개인정보보호 규제 컴플라이언스 수준을 높이는 기회로 활용할 필요

○ 5억 명의 소비자들로 이루어진 유럽시장 진출을 위해 GDPR에 부합하도록 관련 제도를 정비하고 기업 차원의 대응체계를 완비하는 것이 바람직

○ GDPR의 확산성이 높을 것으로 전망되는바, 이를 계기로 개인정보의 수집과 이용에 있어 투명성과 일관성을 담보함으로써 기업과 소비자간 신뢰를 구축하고 유지하는 것은 물론, 지속적인 기업 성장의 발판으로 삼을 필요

– 기업은 규제대응력을 높임으로써 브랜드 가치를 높일 수 있고, 정보주체의 권리를 보호하는데 선도적인 역할을 하고 있다는 평판을 쌓을 수 있음.

① 개인정보 보호는 기업 활동의 기본인프라

○ 수동적인 보호(규제 준수) 차원에서 나아가, 개인정보 보호는 혁신의 기초 역량이라는 시각이 요구

– 개인정보 보호역량은 기업 경쟁력과 혁신역량의 핵심일 뿐만 아니라, 기업에 대한 신뢰도를 향상시키는 등 긍정적인 요소로 작용*

* 사례 1: 영국 소비자를 대상으로 한 설문조사에 의하면, 개인정보 제공이 필요한 거래에서 기업에 대한 신뢰도가 경제적 동기(저렴한 상품 구매 등)보다 더 중요하게 작용(DMA 2018)

* 사례 2: 한국 20대 대학생을 대상으로 한 설문조사에 따르면, 인지도가 낮은 중소기업일수록 공신력 있는 개인정보보호인증마크를 활용하는 것이 온라인에서 소비자의 신뢰를 구축하여 기업가치를 높일 수 있는 효과적인 방법(이화옥 2014)

– 개인정보 보호는 특정 산업·분야의 문제가 아니라, 소비자와의 접점을 형성하는 모든 분야에 해당될 수 있다는 인식이 요구

○ 국내외 인증제도를 활용하여 개인정보 보호 역량 강화

– 국내 각종 개인정 보호 인증* 취득

* 국내에서는 ISMS, PIMS(과기정통부/한국인터넷진흥원), ePrivacy, I-Safe(개인정보보호협회) 등 개인정보 보호 관련 인증 제도가 운영 중

- 해외활동을 위해 ISO 20071* 획득이 필수조건이며, GDPR 이행에도 기여[32)]
  * ISO 27001 인증은 정보보호 분야의 가장 권위 있는 국제 인증으로, 국제표준기구(International Organization for Standards)가 정보보호정책, 통신·운영, 접근통제, 정보보호사고 대응 등 정보보호 관리 11개 영역, 133개 항목에 대해 평가하고 인증 부여

○ '개인정보 보호 적용설계 및 기본설정(Privacy by design and by default)'프레임워크를 도입하는 방안(이하 한국인터넷진흥원 2018).

- IT 시스템, 네트워크로 연결된 인프라, 비즈니스 행태의 설계와 운영 시 프라이버시 보호를 선제적으로 내재화하는 프레임워크를 지칭

- GDPR은 개인정보 보호 적용설계 및 기본설정을 개인정보 처리자 및 수탁자의 법적 의무로 명시
  * GDPR의 '개인정보보호 적용 설계 및 기본 설정'은 개인정보 최소화 및 가명화 방식 등 기술적, 관리적으로 적용 가능한 보호조치를 예로 언급

- '개인정보 보호 적용 설계'는 국내 개인정보 보호법에도 그 기본정신이 반영되어 있음.

- 개인정보보호 적용 설계를 이행할 경우 기술·관리적 보호조치 비용이 발생하지만, 프라이버시를 보호함으로써 얻는 이익과 신뢰 역시 큼.

○ GDPR에서 제시된 개인정보 영향평가(DPIA)의 선제적 도입 검토

- GDPR은 자연인의 권리 및 자유에 대한 고위험을 초래할 가능성이 있을 때 개인정보 영향평가를 요구

- 인공지능 등을 통한 프로파일링이 확산되고, 자동화된 처리에 근거한 광범위한 평가가 해당 정보주체에게 막대한 영향을 미칠 전망

- 국내는 현재 공공부문만을 의무적용사항으로 규정하고 있지만, 세계적인 추세에 부합하여 향후 민간분야로 확대될 가능성도 있음.

- 한 번의 평가로 유사한 복수의 처리작업을 일괄적으로 해결 가능하므로, 여러 선택사항을 고려하여 비선제적 도입을 검토할 필요[33)]

32) GDPR의 주요조항별로 ISO 27001과 비교한 내용은 British Assessment Bureau(2016) 참고.
33) 프랑스 개인정보감독기구(CNIL)는 GDPR에서 요구하는 프라이버시 영향평가(PIA, Privacy Impact Assessment)를 수행하는데 도움을 줄 수 있는 오픈소스 기반 소프트웨어 도구를 개발하여 배포. IAPP. 2017. CNIL

○ 기업의 개인정보책임자(DPO) 확보 및 역량 강화

– GDPR은 EU에서 사업하는 기업 중에 개인정보 처리를 바탕으로 핵심 비즈니스를 하는 기업의 경우 반드시 DPO를 두도록 규정

– 기존의 최고정보보호책임자(CISO) 또는 개인정보보호책임자(CPO)는 기술적 측면이 강조되었으나, DPO는 개인정보 처리 구조를 이해하면서 기술 및 법률적 지식도 갖춘 인력

– DPO는 새로운 개인정보보호 규제환경에 체계적으로 대응할 수 있도록 조직을 이끄는 축으로서, 적임자 선임을 통해 기업의 책임성 강화와 정보주체의 권리강화 추세에 부응할 필요

– 전세계적으로 DPO 인력난이 나타날 수 있어,* 서비스형 DPO[34] 체계 도입 등 기업별 수요에 따른 선제적 대응이 필요

* 프라이버시 전문그룹인 IAPP의 조사에 따르면, GDPR 시행과 더불어 전 세계적으로 7,500여명의 DPO가 추가적으로 필요할 것으로 예측[35]

② 개인정보 보호는 산업 생태계 참여자 모두의 문제

○ 데이터 혁신은 내부 역량만으로 달성하기 어려운 과제로서, 기술 개발·물색, 새로운 분야·제품과의 결합, 글로벌 플랫폼과의 제휴, 데이터 분석 등 국내외의 외부역량 활용이 동반되는 경우가 많음.

○ GDPR이 보여주고 있듯이, 다양한 참여자가 연계된 가치 네트워크 구조에서는 개별 기업이 홀로 정보 보안을 책임지기 어려움.

○ GVC의 성숙과 더불어 해외 협력업체의 정보 보안 관리가 해당 기업의 정보 보호 수준에 영향을 줌.

– ICT와 네트워크가 활성화된 기업은 공급자, 외주업체, 대리점 등의 네트워

releases PIA software for the GDPR: Here's how it works. https://iapp.org/news/a/cnil-releases-pia-software-for-the-gdpr-heres-how-it-works/

34) 세계적인 인력난에 따라 가상 DPO(Virtual DPO) 또는 서비스형 DPO(DPO-as-a-service) 등의 활용성 검토 필요. Info-Security Magazine. 2018. "DPO-as-a-Service Options Pop Up as GDPR Deadline Looms." https://www.infosecurity-magazine.com/news/dpoasaservice-options-pop-up-gdpr/

35) IAPP. 2017. "Study: GDPR's global reach to require at least 75,000 DPOs worldwide." https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/

크와 시스템을 활용한 해커의 공격이 가장 빈번

○ 따라서 한 기업의 내부통제 영역에 대한 보호만으로는 한계가 있으며, 공급 파트너가 되기 위해서는 보안 조치에 대한 상호 계약 합의 등이 요구(이상 김범수·이애리 2017)

③ 관련 전문가, 정부 및 유관기관과의 긴밀한 협력 관계 구축

○ GDPR 등 새로운 개인정보 보호법이 실제적으로 어떻게 적용될지는 많은 부분이 미지수로 남아 있는바, 전문가, 정부, 유관기관과의 협력이 필수적

– 우선, GDPR과 관련된 다양한 국내외 가이드라인[36], 핸드북 등을 참고하여 규정 적용여부 검토, DPO 선임, 유효한 정보주체의 동의 확보, 권리보장, 정보유출 대응 및 피해구제 등 대응방안을 마련

○ 기업과 정부, 유관기관이 협력하여 산업·업종별 개인정보 활용 가이드라인(Code of Conduct)* 준비를 서두를 필요

* GDPR 40(9)는 산업별 개인정보 활용가이드라인 공표와 관련된 조항 포함

– 기존 개인정보 보호법이 사물인터넷, 클라우드, 블록체인 등 새로운 기술을 포괄하지 못할 경우, 기업의 관련 제도·정책에 대한 의견 개진이 매우 중요

– 개인정보 활용 가이드를 활용하여 신기술과 법의 괴리를 해소하여 개인정보 활용의 유연성을 확보하고, 정보주체의 권리 보장

다. 정부의 대응방안

□ GDPR에 대한 인식은 전세계적으로 아직 낮은 수준으로서, 준비도 미흡한 것으로 파악됨.

36) 한국인터넷진흥원(KISA)가 발간한 GDPR 가이드는 개인정보보호 종합포털에서 확인 가능함(https://www.privacy.go.kr).
EU 29조 작업반, 유럽집행위가 제시하는 GDPR 세부 가이드에 대해서는 다음 웹사이트 참고.
European Commission. Article 29 Neswroom. http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360 European Commission. European Commission. 2018 reform of EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

○ 글로벌 IT 시장조사 기관 ESG가 세계 700여명의 사이버보안 및 IT 전문가를 대상으로 조사한 결과, 응답자의 11%만이 GDPR에 완벽히 대응, 33%가 72시간 내 사고 보고 규정을 준수한다고 응답(Oltsik 2018)

○ IT 시장조사기업 Forrester의 조사결과, GDPR의 영향을 받는 기업 중 80%가 법 시행 전까지 규정에 제대로 대응하지 못할 전망(Bristow 2017)

□ GDPR은 글로벌 기업활동 환경에 현저한 변화를 가져올 주요한 사안으로서, 정부의 적극적인 대응이 필수적

① 기업의 개인정보 보호에 대한 인식을 높이는 작업이 우선 중요

○ 각종 행사, 세미나, 교육사업을 통해 국내 개인정보 보호 관련법, GDPR 등 국외 법규에 대해 기업, 유관기관 등의 이해 제고

– EU 집행위원회는 2018~20년간 각 회원국이 실시 중인 홍보·교육사업에 2백만 유로 지원

○ 분야별 개인정보 보호 가이드라인을 발간하고, 기업의 피드백을 받아 지속적으로 개선

② 산업별 영향 모니터링 체제 구축, 기업과의 적극적인 소통과 지원

○ 중견·중소기업, 스타트업을 대상으로 웹페이지 운영을 통해 국내외 개인정보 보호법의 동향과 쟁점 등 확산

○ **기업의 법률 자문 수요에 대한 지원** 등

– GDPR은 실제 적용에 따른 의문사항이 여전히 남아 있어 특히 시행 초기에는 기업들의 자문 수요가 클 전망

○ **국내외 개인정보 보호법의 산업·분야별 영향을 주기적으로 모니터링**

– 정보 보호 관련된 새로운 쟁점이 등장할 가능성이 높은바, 기업에 대한 지

속적인 모니터링을 통해 기민한 대응 요구

③ EU 적정성 평가의 적극적인 추진

○ 적정성 평가를 통과할 경우, EU 시민의 개인정보의 국내 전송·처리 절차가 줄어들어 우리 기업의 부담 완화(그림 III-4 참고)

④ 데이터의 보호와 활용은 국가전략의 일부

○ 데이터를 활용을 촉진할 수 있는 규제 완화

– 예컨대, 우리나라는 비식별정보의 활용을 제한적으로만 허용하고 있어 빅데이터 발전에 제약 요인으로 작용

– 또한 바이오정보와 같이 민감하지만 경제적 잠재력이 큰 분야에 대한 법적 정비를 서두를 필요[37]

○ 우리나라는 개인정보의 국외 이전 시 정보주체의 사전 동의에 전적으로 의존하고 있어 이를 대체할 수 있는 방법을 도입할 필요

– GDPR은 좋은 참고가 되는바, 적정성 평가, 국외이전 표준계약, 구속력 있는 기업규칙 등 동의를 대체할 수 있는 방안 도입이 필요

37) 보다 상세한 내용은 한국인터넷진흥원(2018) 참고.

참고문헌

<국·영문 자료>

김범수·이애리. 2017. 「정보보호」. 김은·김미정 外 10인. 2017. 『4차산업혁명과 제조업의 귀환』. 클라우드나인.

김정곤·나승권·장종문·이성희·이민영. 2015. 『국제 디지털 상거래의 주요 쟁점과 한국의 대응방안』. 대외경제정책연구원.

김정곤. 2017. 「EU 디지털 단일시장 전략의 평가와 시사점」. Global Strategy Report 17-010. 대한무역투자진흥공사.

이화옥. 2014. 『개인정보보호인증마크화 기업에 대한 소비자 신뢰: 브랜드 인지도의 조절효과를 중심으로』. 서울대학교 대학원 학위논문(석사).

한국인터넷진흥원, 2017.2~2018.3. 「해외개인정보동향보고서」.

_____. 2018. 「2018 개인정보보호 7대 이슈 전망」.

창업진흥원. 2017. 『2016년 창업기업 실태조사』. 중소기업청.

행정안전부·한국인터넷진흥원. 2017. 「우리기업을 위한 유럽일반개인정보보호법(GDPR) 안내서」.

_____. 2017. 「우리기업을 위한 유럽일반개인정보보호법 1차 가이드라인」.

Article 29 Data Protection Working Party. 2016. "Guideline on Data Protection Officers(DPO)". European Commission.

BSA. 2018. "2018 BSA Global Cloud Computing Scoreboard: Powering A Bright Future."

British Assessment Bureau. 2016. "GDPR & ISO 27001 Mapping Table."

Business Roundtable. 2015. "Putting Data to Work: Maximizing the Value of Information in an Interconnected World."

Christensen, Laurits, Andrea Colciago, Federico Etro and Greg Rafert. 2013. "The Impact of the Data Protection Regulation in the EU", Intertic Policy Paper, February 2013.

Deloitte. 2013. “Economic Impact Assessment of the Proposed European Geenral Data Protection Regulation.”

DMA. 2018. “Data privacy: What the consumer really thinks.”

ECIPE. 2013. “The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce.”

European Commission. 2012. “How will the EU’s data reform will benefit European businesses?”

European Commission. 2015. “Data protection Eurobarometer: Factsheet.”

ICO. 2017a. “Overview of the General Data Protection Regulation.”

_____. 2017b. “Preparing for the General Data Protection Regulation(GDPR): 12 steps to take now.”

London Economics. 2017. “Analysis of the Potential Economic Impact of GDPR: Implications of the ICO’s Draft Guidelines on Consent.”

Startup Genome. 2017. *Global Startup Ecosystem Report 2017*.

<인터넷 자료>

한국인터넷진흥원. 개인정보보호 종합포털. https://www.privacy.go.kr/

Bavarian Data Protection Agency(BayLDA). EU General Data Protection Regulation. https://www.lda.bayern.de/en/privacy_eu.html

Bristow, Collyer. 2017. “GDPR and Enhanced Individual Rights: A threat or opportunity for organizations?” https://www.lexology.com/library/detail.aspx?g=353b4336-657f-4db7-a13d-ba06e3881bdb

CPVP(Commission for the Protection of Privacy, Belgium). PRÉPAREZ-VOUS EN 13 ÉTAPES.
https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf (검색일: 2018.3.2.)

CNIL. RGPD: se preparer en 6 etapes.

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes (검색일: 2018.2.24.)

MyDataTrust. 2017. "Getting to Know How to Transfer Data to the United States." https://www.mydata-trust.eu/single-post/2017/06/16/GETTING-TO-KNOW-HOW-TO-TRANSFER-DATA-TO-THE-UNITED-STATES (검색일: 2018.5.2.)

European Commission. 2018 reform of EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (검색일: 2018.3.11.)

European Commission. Article 29 Newsroom. http://ec.europa.eu/newsroom/article29/news-overview.cfm. (검색일: 2018.3.10.).

IAPP. 2017. "CNIL releases PIA software for the GDPR: Here's how it works." https://iapp.org/news/a/cnil-releases-pia-software-for-the-gdpr-heres-how-it-works/ (검색일: 2018.3.2.)

IAPP. 2017. "Study: GDPR's global reach to require at least 75,000 DPOs worldwide." https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide (검색일: 2018.3.24.)

ICO. GDPR preparation for Small organisations. https://ico.org.uk/for-organisations/business/

_____. GDPR consent guidance. https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/ (검색일:2018.3.2.)

Info-Security Magazine. 2018. "DPO-as-a-Service Options Pop Up as GDPR Deadline Looms." https://www.infosecurity-magazine.com/news/dpoasaservice-options-pop-up-gdpr/ (검색일: 2018.3.24.)

IT Pro. UK data watchdog draws up plans for 'data protection by design'. http://www.itpro.co.uk/general-data-protection-regulation-gdpr/30694/uk-data-watchdog-draws-up-plans-for-data-protection-by

Lexology. Switzerland to Overhaul its Data Protection Framework. https://www.lexology.com/library/detail.aspx?g=fe5bd158-c73c-4721-bb28-7ff4c604855a (검색일: 2018.3.11.)

Scott, Mark and Laurens Cerulus. 2018. "Europe's new data protection rules export privacy standards worldwide." Politico 웹페이지. https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation

Startup Hubs Europe 웹페이지. http://www.startuphubs.eu

<통계·지표>

수출입은행. 해외투자통계.

통계청. 대륙별·국가별 기업규모별 수출 통계.

한국무역협회. 무역통계(K-Stat).

한국은행. 서비스 국제수지 통계.

<유럽연합 공식문서>

European Commission. 2012. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation), COM(2012) 11 final.

European Union. 2016. 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)

2018년 KOTRA 발간자료 목록

□ GMR (Global Market Report)

번 호	제 목	번호부여일
18-001	유럽 의료기기 시장동향 및 진출전략	2018.1
18-002	중남미 의료기기 시장동향과 우리기업 진출전략	2018.1
18-003	유럽 소비재 유통시장 진출 가이드	2018.1
18-004	한눈에 보는 수출유망국 (의료기기 ③편)	2018.1
18-005	2017년 하반기 수입규제 동향과 2018년 상반기 전망	2018.1
18-007	글로벌 로봇산업 시장동향 및 진출방안	2018.2
18-008	4차 산업혁명 관련 신산업 해외경쟁력 설문조사 분석	2018.3
18-009	글로벌 가공식품 시장동향과 우리기업 진출전략	2018.3
18-010	아프리카 의료기기 시장동향과 우리기업 진출전략	2018.3
18-011	글로벌 메가시티 히트상품-패션	2018.3
18-012	GCC 및 이란 중소기업 수출유망품목과 주요 인증제도	2018.4
18-013	4차 산업혁명 글로벌 트렌드 리포트 - CES 2018에서 본 소비, 일자리, 조직문화의 혁신	2018.4

□ GSR (Global Strategy Report)

번 호	제 목	번호부여일
18-001	러시아 극동지역 주요산업 협력방안	2018.3

□ KOCHI자료

번 호	제 목	번호부여일
18-001	2017년 대중수출 성과와 2018년 전망	2018.1
18-002	중국 서비스산업의 부상과 진출 확대 방안	2018.4
18-003	양회에 나타난 중국의 2018년 경제정책과 시사점	2018.4

□ GIP (Global Issue Paper)

번 호	제 목	번호부여일
18-001	이란 핵합의 현황 점검과 우리기업 대응방안	2018.1

□ GTR (Global Trade Report)

번 호	제 목	번호부여일
18-001	2017년 12월(연간) 수출 동향	2018.1
18-002	2018년 1월 수출 동향	2018.2
18-003	2018년 2월 수출 동향	2018.3
18-004	2018년 2분기 KOTRA 수출선행지수	2018.3
18-005	2018년 3월 수출 동향	2018.4

□ KOTRA자료

번 호	제 목	번호부여일
18-001	동남아 대양주 프랜차이즈 시장동향	2018.1
18-002	한눈에 보는 해외 25개국 취업정보	2018.1
18-003	월드챔프 성공사례집: 2017년 코트라 월드챔프사업 참가기업의 수출 성공스토리	2018.2
18-004	2018-2019 해외전시회 한국관 디렉토리	2018.3
18-005	2017 KOTRA 글로벌 CSR 종합보고서	2018.3
18-006	해외에서 더 가까이 FTA 활용을 도와주는 FTA 해외활용지원센터 활동사례집	2018.3
18-007	2017 외국인투자옴부즈만 연차보고서	2018.3
18-008	Foreign Investment Ombudsman Annual Report 2017	2018.3
18-009	2017 IP-DESK 백서	2018.3
18-010	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 러시아 RUSSEZ : RUSSEZ 발전 전략 수립을 위한 정책 제언	2018.3
18-011	2016/17 Knowledge Sharing Program(Industry&Trade) with Russia RUSSEZ : Consulting for the Development of Russian Special Economic Zones(RUSSEZ)	2018.3
18-012	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 러시아 연해주 : 루스키섬 개발 전략 및 투자 유치 방안	2018.3
18-013	2016/17 Knowledge Sharing Program(Industry&Trade) with Russia Primorsky Krai : Russky Island Development Strategy and Investment Promotion Plan	2018.3

18-014	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 미얀마 : 미얀마 대외무역투자 증진방안	2018.3
18-015	2016/17 Knowledge Sharing Program(Industry&Trade) with Myanmar : Policy Recommendations for Industry, Trade and Investment Promotion in Myanmar	2018.3
18-016	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 우즈베키스탄 : 섬유산업 발전을 위한 정책 수립 방안	2018.3
18-017	2016/17 Knowledge Sharing Program(Industry&Trade) with Uzbekistan : Policy Consultation for the Development of the Textile Industry in Uzbekistan	2018.3
18-018	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 이란 1 : 이란의 외국인투자 유치 확대방안 : OIETAI의 역량강화를 위한 정책적 제언	2018.3
18-019	2016/17 Knowledge Sharing Program(Industry&Trade) with Iran 1 : Policy Recommendations for Capacity Building for OIETAI in Promotion of FDI to Iran	2018.3
18-020	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 이란 2 : 이란 ICT 연구개발센터 발전방안 수립	2018.3
18-021	2016/17 Knowledge Sharing Program(Industry&Trade) with Iran 2 : Securing the Means for the Development of the Iranian ICT R&D Center	2018.3
18-022	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 칠레 : 칠레 만성질환 환자를 위한 원격의료 컨설팅 및 모델링 디자인	2018.3
18-023	2016/17 Knowledge Sharing Program(Industry&Trade) with Chile : Consulta de Políticas sobre Telemedicina Domiciliaria y Diseño de Modelos de Telemedicina para Enfermedades Crónicas en Chile	2018.3
18-024	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 케냐 : 케냐의 산업단지 개발 계획 수립	2018.3
18-025	2016/17 Knowledge Sharing Program(Industry&Trade) with Kenya : Policy Recommendations for Development Plan of an Industrial Park in Kenya	2018.3
18-026	2016/17 경제발전경험 공유사업(KSP) 산업&무역 정책자문 쿠바 : 쿠바의 신재생에너지 발전 역량강화	2018.3
18-027	2016/17 Knowledge Sharing Program(Industry&Trade) with Cuba : Capacity Building for Development of the Renewable Energy & Industrial Sectors in Cuba	2018.3
18-028	세계시장, 문을 열면 희망이 보인다: 온라인마케팅·무역사절단·지방지원단 특화사업 우수사례	2018.3
18-029	지사화 우수사례집: 2017 코트라 지사화사업을 통한 20개 기업의 수출 성공스토리	2018.3
18-030	서비스산업 해외진출 성공사례	2018.4
18-031	주요국별 경제통계 가이드북	2018.4
18-032	SEOUL FOOD 2018 디렉토리	2018.4

□ 설명회자료

번 호	제 목	번호부여일
18-001	2018 세계시장 진출전략 설명회	2018.1
18-002	2018 방산·보안기업 지원 사업설명회	2018.2
18-003	KSP(Knowledge Sharing Program)연계 멕시코 KSP 에너지·바이오·IT 진출전략세미나	2018.2
18-004	바다로! 대륙으로! 시장을 넓혀라!, 아세안·인도·유라시아 진출 설명회	2018.2
18-005	KOTRA 해외수주협의회 제 31차 수요포럼: 해외 체류시 재난 및 안전 대응 방안	2018.3
18-006	2018 UN 공공조달 플라자 (UN Procurement Plaza 2018)	2018.3
18-007	홍콩의 금융-무역 플랫폼을 활용한 해외시장 진출 설명회	2018.3
18-008	미국 투자환경 설명회	2018.4
18-009	Global Project Plaza 2018	2018.4
18-010	중국 서비스 수출병법	2018.4
18-011	FTA를 활용한 중남미 진출전략 설명회	2018.4

작성자

◈ 글로벌전략지원단 김정곤
◈ 한국인터넷진흥원 윤재석

Global Strategy Report 18-002

EU의 일반개인정보보호법 발효와 대응과제

발 행 인 | 권평오
발 행 처 | KOTRA
발 행 일 | 2018년 5월
주 소 | 서울시 서초구 헌릉로 13 (06792)
전 화 | 02) 1600-7119(대표)
홈페이지 | www.kotra.or.kr
문 의 처 | 글로벌전략지원단 (02-3460-3368)

ISBN : 979-11-6097-713-4 (95320)

Global Strategy Report

kotra
Korea Trade-Investment Promotion Agency