Privacy Report 2017.10

SOMANSA

2018년 5월 25일 시행. 과징금 전세계 매출액의 4%

GDPR. 전 유럽연합에 적용되는 개인정보보호법 핵심은 개인정보의 보호와 활용의 〈균형〉

G3(미국, 중국, 유럽연합) 개인정보보호법제 어떤 변화가 일어나고 있나?

유럽연합 28개국 대상. 23년만의 변화. GDPR

General Data Protection Regulation의 약자로
유럽연합 28개국에 적용되는 강화된 개인정보보호법.
1995년 제정되어 23년간 이어져온 유럽연합 개인정보보호지침을 대체

EU 거주자에게 제품 or 서비스 제공시 GDPR 적용대상

- EU내 법인이 설립되어 있는 경우 적용
- (EU에 법인이 없어도) 거주자에게 제품이나 서비스를 하는 경우 적용
- EU 거주자의 행동을 모니터링하는 경우 적용

핵심은 개인정보보호와 활용의 균형

정보의 수집 및 공유 규모가 상당한 수준으로 확대되었다. 기술을 통해 민간기업과 공공기관이 업무수행을 위해 전례 없는 규모로 개인정보를 활용하게 되었다. 개인은 개인정보를 공적으로 세계적으로 활용할 수 있다. 기술은 경제와 사회생활을 변화시켜왔다. 앞으로는 기술을 통해 유럽 역내의 자유로운 정보 이동과 제 3국 및 국제기구로의 개인정보 이전을 용이하게 하고, 개인정보를 높은 수준으로 보호해야 한다.

효과적인 협력을 보장하기 위해서 필요하다. 역내시장이 적절하게 기능을 발휘하기 위하여는 개인정보처리 관련 개인보호와 연계되었다는 이유로 유럽연합 내 개인정보의 자유로운 이동을 제재하거나 금지하지 않아야 한다. 영세 및 중소기업의 특정 상황을 고려하기 위해,

(4) 개인정보처리는 인류에 기여할 수 있도록 설계되어야 한다. 개인정보보호권은 절대적 권리가 아니며, 개인정보보호권은 사회에서의 개인정보보호 기능과 관련하여 고려되어야 하며 비례의 원칙에 입각하여 다른 기본권과 균형을 이루어야 한다. 이 법은 모든 기본권을 존중

- GDPR원문 중 발췌
- 개인정보의 활용과 자유로운 이동
  과학기술발전 및 활용에 개방적

1. 어떤 정보가 GDPR의 주된 보호대상인가?

신기술을 반영하는 정보와 유전자정보, 건강관련정보에 Focus

(30) 개인기기, 어플리케이션, 인터넷 프로토콜 주소, 쿠키정보, 전파식별태그 등, 기타 식별인자와 같은 툴(tool)과 프로토콜(protocol)이 제공하는 온라인식별인자로 인해 개인이 연결될 수 있다

(34) 유전자정보는 개인의 유전적 또는 후천적으로 얻은 유전자특성에 관한 개인정보로 정의, 중략

(35) 건강관련 개인정보에는 정보주체의 과거, 현재, 혹은 미래의 신체적 또는 정신적 건강 상태의 정보를 드러내는 모든 정보주체의 건강상태에 속하는 정보가 포함, 중략

자동화 구조화 연결

GDPR 보호 대상은 〈자동화, 구조화 된 정보〉

1 (DB,WAS, Server등 시스템에서) **자동화처리 되는 정보**

+ **2** 자동화처리 되지 않더라도 구조화된 파일링시스템

기준에 따라 정렬되지 않은 개인정보에 대한 커버페이지, 파일, 파일세트에는 비적용

BIG DATA

빅데이터 축적

가장 중요한 보호 대상은 〈프로파일링〉

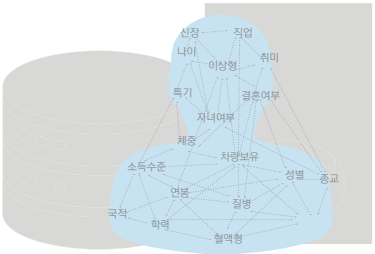
프로파일링의 조건

1. 평가와 예측 목적

2. 인적개입 없이 자동화처리

인적개입없이 시스템으로 자동화처리하여

빅데이터가 융합하여 →  → 평가, 예측이 가능하도록 프로파일링



(30) 개인기기, 어플리케이션, IP주소, 쿠키정보, 전파식별태그 등, 기타 식별인자와 같은 툴(tool)과 프로토콜(protocol)이 제공하는 온라인식별인자로 인해 개인이 연결될 수 있다. **특히 이러한 정보는 개인에 대한 자취를 남겨, 이러한 정보가 서버를 통해 전해지는 독특한 식별인자 및 기타정보와 결합되는 경우, 해당 개인에 대한 프로파일을 생성하고 이들을 식별하는 데 사용될 수 있다.**

예) EU 거주자를 Stylometry를 사용 프로파일링할 경우 규제대상이 될 수 있음

실제 주타겟은 구글, 페이스북, 아마존 등 글로벌웹서비스제공자가 될 확률이 높음

〈Stylometry〉
비트코인의 창시자 사토시나카모토를 미국 NSA에서 찾아낸 방법.
구글, 야후 , 아마존, 페이스북 등의 데이터를 빅데이터분석, 수치화하여 사토시나카모토의 스타일을 프로파일링한 후 그를 식별함

2. GDPR의 핵심은 개인정보보호와 활용의 균형

개인정보의 보호측면 | 개인정보의 활용측면

개인정보의 보호 | 개인정보의 활용

〈보호대상〉 자동화, 구조화된 개인정보

(DB, WAS, Server 등 시스템에서)
자동화처리되는 개인정보

활용측면 의미

기준에 따라 정렬되지 않은 개인정보페이지 파일까지 식별 및 분석하지 않아도 되므로 기업 측 리소스 감소

〈가장 중요한 보호대상〉평가, 예측목적으로 인적개입없이 자동화생성한 프로파일링

보호측면 의미

온라인상 자취를 다른 정보와 결합하여 인간 자체를 정의하는 프로파일링을 최초 규제.
향후, 사물인터넷시대의 정보유출을 대비

프로파일링에 대한 정보주체의 권리

1. 프로파일링에만 근거한 결정을 거부할 권리
예) 온라인신용평가를 자동거절, 전자채용을 거절하고 인적개입을 요구
2. 프로파일링처리를 반대할 권리
3. 프로파일링로직에 관한 의미있는정보를 제공받을 권리

프로파일링에 대한 기업 측 보호조치

1. 광범위한 프로파일링 처리시 영향평가
2. 적절한 로직을 사용
3. 적절한 기술적조직적조치
4.차별이 발생하지 않도록 보호

활용측면 의미

핵심보호대상인 프로파일링 DB 및 연계시스템에 보안리소스 집중가능

〈준수 입증수단〉 Privacy By Design (Data protection by design and by default)

보호측면 의미

초기부터, 전체 라이프사이클에 걸쳐 개인정보를 보호받을 수 있음

모든 프로젝트초기부터, 전체 라이프사이클에 걸쳐 개인정보보호권장
컨트롤러가 Privacy By Design을 위해 시행해야하는 5대 조치

① 개인정보처리의 최소화 ②빠른 시일내 개인정보가명처리
③ 개인정보의기능및처리의투명 ④ 정보주체의 개인정보처리에 대한 감시
⑤정보처리자의 보안대책 수립 및 개선

활용측면 의미

가명화처리를 하면 활용범위 넓어짐

정보주체의 권리 강화

보호측면 의미

삭제권으로 잊혀질 권리를 명시.

이동권으로 구조화된 개인정보를 경쟁사에 직접 전송해야하는 상황도 가능해짐

〈개인정보 삭제권〉(잊혀질 권리)

기업기관의 업무

포탈은 다른 관련사이트에게 링크, 복제정보까지 파기하라고 요청해야함

〈개인정보이동권〉

개인정보를 다른 서비스에 재사용할 수 있도록 개인정보의 이동을 요구할 수 있는 권리

기업기관의 업무

1. 기계판독이 가능한 형태로 제공
2. 이전요구시 1개월 이내에 조치
3. 인증, 암호화 등 보안적용
4. 요구시 다른 컨트롤러에게 직접전송

〈대표적 보호조치〉 가명처리

추가정보 없이는 식별할 수 없게 처리하는 것으로 추가정보는 분리보관하고, 기술적/조직적 조치를 취해야 함

활용측면 의미

- 비식별화처리에 비해 단순한 방식인 가명처리로 동의받은 목적외로 활용을 허용함
- GDPR은 과학, 의학 등 신기술에 매우 우호적이며 개인정보를 가명화처리하여 활용할수있도록 함

〈처벌〉 과징금 전세계 매출의 4% 까지 확대

중대위반시 : 과징금 전세계매출 4% or 2천만유로 ,
일반위반시 : 과징금 전세계매출 2%or 1천만 유로 중 높은 금액

형사처벌 규정 없음

3. 개인정보보호법과 GDPR의 비교

구분	개인정보보호법	GDPR
법의 목적	**개인정보의 보호** 개인정보의 수집 · 이용, 제공 등 개인정보 처리 기본원칙, 개인정보의 처리 절차 및 방법, 개인정보 처리의 제한, 개인정보의 안전한 처리를 위한 관리 · 감독, 정보주체의 권리, 개인정보권리 침해에 대한 구제 등에 대하여 규정	**개인정보의 활용과 보호의 균형** 자유, 안보 및 정의와 경제 연합 분야의 성과, 경제 및 사회적 발전, 역내 시장경제의 강화 및 통합, 그리고 개인의 복지 증진
물적 허용범위	**개인을 식별할수 있는 정보** 정보의 내용 · 형태 등은 특별한 제한이 없고 개인을 알아볼 수 있는 모든 정보가 개인정보가 될 수 있음. 즉, 디지털형태나 수기형태, 자동처리나 수동처리 등 그 형태 또는 처리방식과 관계없이 모두 개인정보에 해당	**자동화 구조화된 개인정보에 적용** 개인정보를 처리하는 '자동화된시스템(automated systems)과 구조화된 개인정보 파일링시스템에 적용됨
정보주체가 행사할 수 있는 권리	**열람, 정정 · 삭제, 처리정지, 손해배상청구등** 개인정보의 열람, 정정 · 삭제, 처리정지, 손해배상 청구 등	**잊혀질권리, 이동권, 프로파일링 관련 권리** 정보주체의 열람권, 정정권, 삭제권(잊혀질권리), 처리제한권, 이동권, 반대할 권리, 자동화된 결정 및 프로파일링 관련 권리 등
동의목적외 활용조건	**비식별화시 활용가능** 〈비식별화〉시 동의목적 외 활용가능	**가명화시 활용가능** 추가정보 없이 식별할 수 없게 하고 추가정보를 분리보관하여 기술적 조직적조치를 취할 경우 동의목적외 활용가능
프로파일링 규정	없음	**개인을 평가하는 프로파일링은 GDPR의 핵심 조항** 프로파일링의 개념 : 평가와 예측 목적으로 인적 개입 없이 자동화처리하는 정보
과징금	**매출의 최대 3% 과징금** -매출의 최대 3% 과징금 -주민번호 유출시 과징금 5억원 징수	**전세계 매출4% 또는 2천만유로** -중대위반: 최대 전세계 매출 4% 또는 2천만 유로중 높은금액 -일반위반사항: 전세계 매출 2% 또는 1천만 유로중 높은금액
형사처벌	**형사처벌 수위가 높음** 2년 이하 징역 or 2천만원 이하 벌금형 선고 위반행위로 취득된 금품이나 이익은 몰수 · 추징 대상	없음

4. 우리기업의 GDPR 준비방향

1단계

EU에 사업장이 있고 사업장에서 개인정보를 처리하는가
사업장 : 자회사, 본점 무관. 일정한 조치를 통해 실질적 활동을 수행

OR

EU 거주 개인정보주체에게 재화와 서비스를 제공하는가
(고객 정보 확인) 또는 EU 내 정보주체에 대해 EU 내 행동을 모니터링 하는가
제공 여부 : 단순히 웹사이트를 제작하여 인터넷에 공개한 경우는
서비스 제공으로 보기 어렵고 특정 언어, 통화, 서비스 제공 대상 등이
EU 회원국의 회원을 고객으로 예상하고 있다고 볼 수 있는지 등이 고려됨

NO → GDPR 적용되지 않음

YES

2단계

기술적 · 조직적 보호조치 시행, 약관 · 계약서 수정, 매뉴얼 확립

1 개인정보 취급자 유형 파악 : 컨트롤러* or 프로세서* 인지 확인
■ 각 정보처리 활동 별로 파악: 컨트롤러인지 프로세서인지에 따라 의무가 달라짐
*컨트롤러: 개인정보의 이용 목적과 처리 수단을 결정하는 자
*프로세서: 컨트롤러를 대신하여 개인정보를 처리하는 자

2 DPO 지정(Data protection officer) 및 감독기관에 DPO 인적사항 통보
■ 필수 지정해야 하는 경우
① 컨트롤러 또는 프로세서의 핵심활동이,
1) 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링을 요하는 처리 작업들로 구성되는 경우,
2) 민감정보나 범죄경력 및 범죄 행위 정보의 대규모 처리로 구성되는 경우,
② 공공기관(법원 제외)은 필수 지정
■ 지정 방법 : 각 사업장이 인접한 경우 우 사업자그룹은 한명의 DPO를 공동으로 지정 가능, 외부인 지정 가능 (직원, 서비스 계약을 통한 지정 가능)

3 Data protection by design and by default : 모든 프로젝트 초기 단계에서 개인정보 보호를 중요한 고려사항으로 하고, 전체 라이프사이클에서 전반에 걸쳐 개인정보 보호 권장
예) 개인정보처리의 최소화(data minimisation), 처리에 필요한 보호조치(safeguards), 가명화(pseudonymisation) 등의 적절한 기술적 · 조직적 조치 필요

4 보호조치 수준 결정
■ 민감정보, 프로파일링 처리, 아동의 개인정보 처리시 보호조치 강화

5 프로세서와 서브프로세서 관리
■ 개인정보처리 위탁 등 계약서는 반드시 문서화, 프로세서와 서브프로세서의 정보보호수준을 계약 전 확인, 계약서에 협력사의 정보보호의무 명시

6 약관에 개인정보주체의 정보이전권, 프로파일링 등
자동화된 의사결정에 관한 처리 제한권 등 개인정보주체의 권리 및 행사 방법 명시

7 EU 밖으로 개인정보 이전시 사안별로 조치 방법 확인

8 개인정보영향평가 (DPIA, Data Protection Impact Assessment) 실시 검토

9 행동강령 (Codes of conduct) 채택

10 정보 유출시 [국가별 감독기관]에 72시간 이내 통지 및 정보주체에게 지체없이 통지

5. (우리나라로) EU국민 개인정보 이전시 조치

이전 유형별 구분		요 건	처벌
(제45조) 적절성결정에 따른 제 3국 이전		[집행위원회]가 [제3국], [해당 제3국의 영토나 하나 이상의 지정 부문], [국제기구]가 적정한 보호수준을 제공한다고 보아 적절하다고 결정하는 경우	과징금 전세계 매출액의 4% 또는 2천만 유로
컨트롤러나 프로세서의 보호조치가 적정한 경우 (Appropriate Safeguards)	(제46조) [국가별 감독기관]의 승인 없이 이전가능요건	공공기관 또는 기구 간에 법적 구속력이 있고 강제할 수 있는 장치가 있는 경우	
		제47조에 따른 〈의무적 기업 규칙- binding corporate rules〉	
		[집행위원회]가 채택한 〈표준개인정보보호조항-standard data protection clauses〉	
		[국가별 감독기관]가 채택하고 [집행위원회]가 승인한 〈표준개인정보보호조항-standard data protection clauses〉	
		제40조에 의거 승인된 〈행동강령-approved code of conduct〉	
		제42조에 의거 승인된 〈인증-approved certification〉	
	(제47조) [국가별 감독기관]의 승인 필요경우	[컨트롤러 or 프로세서]와 [제3국 or 국제기구의 컨트롤러 or 프로세서] 사이의 계약조항	
		공공기관 또는 기구 간에 법적 구속력이 있고 강제할 수 있는 장치	
예외 및 기타	(제49조) 이전가능 요건	적절성결정 및 적절한 보호조치가 없음으로 인해 정보주체에게 발생할 수 있는 위험을 고지받은 후 정보주체가 이전에 명시적으로 동의한 경우	
		정보주체와 컨트롤러 사이의 계약 이행을 위해 또는 정보주체의 요청에 의해 취해진 계약전 사전조치의 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 권리 확립, 행사, 수호를 위한 경우	
		정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우 정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위한 경우	
		EU 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 조회하기 위한 목적으로 만들어진 개인정보 기록부(register)로부터 EU 또는 회원국 법률에 명시된 조회의 조건이 충족되는 범위 내에서 이전하는 경우	
	예외	반복적인 이전이 아닐 것, 한정된 숫자의 개인정보 주체의 정보에 대한 이전일 것, 컨트롤러의 정당한 이익을 위해 필요한 전송일 것, 적절한 보호조치에 따른 이전일 것이 모두 만족된 경우 이전 가능 ([국가별 감독기관] 통지는 필수)	

출처: 정보이전권에 관한 가이드라인 요약번역문(개인정보보호위원회)

6. GDPR 보호조치 요구사항 – 기술적 보호조치

<table>
<tr><th colspan="2">구분</th><th>내용</th></tr>
<tr><td colspan="2">기술적 · 관리적 보호 조치
* 세부지침 발표예정</td><td>최신 기술, 이행 비용, 처리의 성격과 범위, 상황, 목적 뿐 아니라
정보주체 권리에 변경이나 중대한 위험을 초래할지 여부를 참작하여 위험에 적합한
보안 수준을 보장하는 〈기술적 · 조직적 보호조치〉 필요 (아래의 조치 필수):

필수적인 〈기술적 · 조직적 보호조치〉
① 개인정보의 가명처리 및 암호처리
② 처리시스템 및 서비스의 지속적 기밀성과 무결성, 유용성, 복원력
③ 물리적 사고나 기술적 사고가 발생하는 경우 신속하게 복원하여 유용성 및 접근 확보
④ 정기적 검사, 평가 및 해당 처리의 보안을 보장하기 위한 기술 및 관리조치의 효용성에 대한 평가</td></tr>
<tr><td rowspan="2">개인정보
영향평가
(DPIA, Data
Protection
Impact
Assessment)
* 세부 지침
발표 예정</td><td>영향평가가
필요한 경우</td><td>[원칙] 컨트롤러가 새로운 기술을 사용하고,
그 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 가능성이 있는 경우
개인정보를 처리하기 이전에 영향평를 수행해야 함

[필수]
1. 프로파일링을 포함한 자동화된 처리에 근거한 자연인에 대한 체계적이고 광범위한 평가로서
해당 평가에 기반한 결정이 해당 정보주체에게 법적 효력을 미치거나
이와 유사하게 중대한 영향을 미치는 경우
2. 민감정보 또는 유죄판결 및 형사범죄에 대한 대규모 처리를 하는 경우
3. 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링(가이드라인의 예 : CCTV)</td></tr>
<tr><td>영향평가 항목
(최소조건)</td><td>1. 예상되는 개인정보처리와 처리목적, 컨트롤러가 추구하는 정당한 이익
2. 처리목적에 대한 처리작업의 필요성과 비례성
3. 정보주체의 권리와 자유에 미치는 위험성 평가
4. 개인정보보호와 GDPR 준수를 입증하기 위한 보안조치(security measures),
보호조치(safeguards) 및 매커니즘(mechanisms) 등 위험방지조치</td></tr>
</table>

출처: 정보이전권에 관한 가이드라인 요약번역문(개인정보보호위원회)

7. GDPR 보호조치 요구사항 – 정보주체 권리보장을 위한 조치

구분	내용
삭제권 개인정보의 삭제를 컨트롤러에게 요구할 권리	컨트롤러는 다음 중의 하나에 해당할 경우 정보주체의 삭제권을 보장: ① 개인정보가 원래의 수집 · 처리 목적에 더 이상 필요하지 않은 경우 ② 정보주체가 동의를 철회한 경우 (단, 해당 처리에 대한 법적인 사유가 없는 경우) ③ 정보주체가 처리에 반대하는 경우로서 처리의 계속을 위한 더 중요한 사유가 없는 경우 ④ 개인정보가 불법적으로 처리된 경우(GDPR 위반 등) ⑤ 법적 의무 준수를 위하여 삭제가 필요한 경우 ⑥ 아동에게 제공할 정보사회서비스와 관련하여 개인정보를 처리한 경우 삭제거부가 가능한 경우: ① 표현 및 정보(information)의 자유에 관한 권리 행사를 위한 경우 ② 공익적 임무의 수행 및 직무권한 행사를 위한 법적 의무 이행을 위한 것인 경우 ③ 공익을 위한 보건 목적을 위한 경우 ④ 공익적 기록보존(archiving purposes), 과학 및 역사적 연구 또는 통계 목적을 위한 것인 경우 ⑤ 법적 청구권의 행사나 방어를 위한 것인 경우
이동권 개인정보를 자신 또는 제3자에게 이전할 것을 요구할 수 있는 권리	개인정보의 이동권은 다음의 경우에 적용: ① 정보주체가 컨트롤러에게 제공한 개인정보 ② 처리가 정보주체의 동의에 근거하거나 계약의 이행을 위한 것 ③ 처리가 자동화된 수단에 의해 이루어지는 경우 처리방법: ① 정보주체의 요구를 받은 때로부터 1개월(요구가 복잡한 경우 사유를 알리고 2개월 연장) 이내 처리 ② 정보가 SW가 추출할수 있는 구조화된 방법으로 제공 (예: CSV 등) ③ 기술적으로 가능하다면 해당 개인정보를 한 컨트롤러 에서 다른 컨트롤러로 직접 전송 ④ 개인정보 이동권으로 인해 지적재산권이나 영업비밀 등 타인의 권리가 침해되는 경우에는 거부가능
자동화된 결정 및 프로파일링 관련 권리 자동화된 개인평가에 대해 적용을 받지 않을 권리	프로파일링 예시: 자동화된 (인적개입 없는) 전자채용 (e-Recruit), 온라인 신용신청 (online credit decision) 컨트롤러가 보장해야할 정보주체의 자동화된 결정 및 프로파일링 관련 권리: ① 인적 개입(human intervention)을 요구할 권리 ② 정보주체가 자신의 관점(point of view)을 표현할 권리 ③ 그 결정에 대한 설명을 요구할 권리 및 그에 반대할 권리

*개인정보에 대한 정보주체의 권리는 절대적인 권리가 아님

8. 개인정보 침해 발생시 조치

침해유형

① 개인정보의 파괴(destruction), ② 손실(loss), ③ 변경(alteration),
④ 인가되지 않은 공개(unauthorised disclosure)을 야기하는 보안 위반(a breach of security)*

통지의무

[국가별 감독기관] 대상 통지

원칙 : 72시간 이내

예외 : 책임성 원칙에 따라 해당 개인정보 침해가 개인의 권리와 자유에 위험을 초래할 가능성이 낮은 점을 컨트롤러가 입증할 수 있어야 예외 인정(전문 제85조), 72시간 경과 후에는 지체된 이유도 통지

개인정보주체에게 통지 : 인지 후 부당한 지체 없이 통지

통지내용

① DPO 및 다른 연락처에 대한 이름 및 상세 연락처,
② 개인정보 침해로 인해 발생할 수 있는 결과,
③ 부작용을 완화할 수 있는 조치 등 컨트롤러가 해결을 위해 취하거나 취하도록 제시된 조치 통지의무 면제 요건

통지의무 면제 요건

① 침해 당시 적절한 기술적 조직적 보호조치를 이행하였고, 피해정보주체에게 해당 조치가 적용된 경우,
② 컨트롤러가 피해 정보주체의 권리와 자유에 높은 위험을 초래할 가능성이 없도록 하는 후속조치가 이루어진 경우,
③ 통지에 과도한 노력이 수반되는 경우 (정보주체가 동등하게 효과적인 방식으로 연락 받을 공적 연락 수단 등 유사한 조치가 있는 경우 통지에 갈음)

문서화 컨트롤러는 침해와 관련된 사실, 그 영향과 취해진 구제조치 등 모든 사항을 기록

통지방법 구체적 내용 없음, 추후 발표될 EU 지침(통지의 형식과 절차에 관한 지침, Data breach notifications) 참고

프로세서의 통지의무

프로세서는 컨트롤러에게 부당한 지체 없이 침해사실을 통지해야 함

문서화 의무: 컨트롤러는 침해와 관련된 사실, 그 영향과 취해진 구제조치 등 모든 사항을 기록

9. 피해 구제 및 제재 규정

<table>
<tr><th colspan="2">구분</th><th>주요내용 및 유의사항</th></tr>
<tr><td rowspan="3">피해구제제도</td><td>[국가별
감독기관]</td><td>정보주체는 [국가별감독기관]에 민원을 제기할 수 있음</td></tr>
<tr><td rowspan="2">사법구제</td><td>자연인 또는 법인은 [국가별감독기관]의 법적구속력있는 결정에 반대하여
법원에 사법구제(judicial remedy)를 신청할 권리가 있음</td></tr>
<tr><td>정보주체는 위반책임이 있는 컨트롤러나 프로세서에 대해 사법구제를 구할 수 있음
(프로세서에게까지도 적용할 수 있다는점 유의, 사업장이 있는 회원국의 법정이 관할)</td></tr>
<tr><td rowspan="3">정보주체에
대한
손해배상</td><td>범위</td><td>금전 및 비금전 손실(non-pecuniary loss)</td></tr>
<tr><td>프로세서도
배상책임부담</td><td>컨트롤러뿐 아니라 프로세서도 손해배상 의무부담:
GDPR의 프로세서에 대한 규정을 자신 또는 서브프로세서의 처리로 인해 위반한 경우,
컨트롤러의 지시사항 위반 또는 지시의 범위를 벗어난 행위로 인해 발생한 손해배상</td></tr>
<tr><td>당사자 관계</td><td>복수의 컨트롤러 또는 프로세서에게 책임이 있는 경우 각 당사자가 손해 전체에 대해 책임
(당사자간 내부 구상은 가능)</td></tr>
<tr><td colspan="2">과징금</td><td>[과징금 부과 원칙]
① 개별사안별로 [국가별감독기관] 결정에 의해 부과됨
② 과징금부과는 유효(effective)하고 비례적이며(proportionate) 설득력(dissuasive) 있어야함
③ 동일사안이 여러규정을 위반하고 있는 경우 장중한 침해에 규정된 과징금 액수를
초과하여 부과 되지않음
④ 과징금액수(최대액수기준):
직전 회계연도의 전세계 매출액의 4% or 2천만유로(한화약250억원)중 더 큰금액
또는 전세계매출액의2% or 1천만유로 중 높은 금액</td></tr>
<tr><td colspan="2">처벌</td><td>회원국은 추가처벌(penalties)을 규정할 수 있기 때문에 회원국별로 처벌수위가 상이할 수있음
(회원국의 법률은 2018. 5. 25. 까지 EU[집행위원회]에 통보되어야 함)</td></tr>
</table>

10. 위반에 따른 과징금 규정

구분		주요내용 및 유의사항	조항
직전 회계 연도의 전세계 매출액의 4% 또는 2천만 유로중 더 큰 금액	동의 등 정보처리의 기본원칙 위반	개인정보처리에 관한 원칙	제5조
		처리의 적법성	제6조
		동의의 조건	제7조
		민감정보 처리	제9조
	정보주체 권리침해	정보주체의 권리행사를 위한 투명한 정보, 통지 및 형식	제12조
		개인정보를 정보주체로부터 수집시 제공 정보	제13조
		정보주체로부터 수집하지 않을 경우 제공 정보	제14조
		정보주체의 열람권	제15조
		수정권	제16조
		삭제권(잊혀질권리)	제17조
		처리에 대한 제한권	제18조
		수정이나 삭제 또는 처리의 제한에 관한 고지의무	제19조
		개인정보 이전권	제20조
		반대할 권리	제21조
		프로파일링을 비롯한 자동 개별 의사결정	제22조
	제3국이나 국제기구의 수령인에게 개인정보이전	국외 이전을 위한 통칙	제44조
		적정성 결정에 따른 이전	제45조
		적절한 안전조치에 의한 이전	제46조
		의무적 기업 규칙	제47조
		유럽연합법률로 인가되지 않은 정보의 이전 또는 공개	제48조
		특정상황을 고려한 적용의 일부 제외	제49조
	제9장에 따라 채택된 회원국 법률에 따른 의무 위반		제9조
	제58조 제2항에 따라 [국가별감독기관]이 내린명령 또는 정보처리의 임시적 또는 확정적 제한, 또는 개인정보 이동의 중지를 준수하지 않거나 열람의 기회를 제공하지 않아 제58조 제1 항을 위반한 경우		제58조

10. 위반에 따른 과징금 규정

구분		주요내용 및 유의사항	조항
직전 회계 연도의 전세계 매출액의 2% 또는 1천만 유로중 더 큰 금액	컨트롤러와 프로세서의 의무 위반	아동(16세미만) 아동의 개인정보 처리시 친권자 동의 필요	제8조
		신원확인이 필요하지 않은 경우 정보주체의 신원확인을 위한 추가정보를 보관 또는 처리하지 않아도 되는데 이 경우 가능하면 정보주체에게 해당 정보주체를 식별할 수 없다는 점을 통지 해야함	제11조
		Data protection by design and by default 원칙준수. 데이터 최소화 등 개인정보보호원칙 이행 및 안전조치를 위한 가명처리 등 적절한 기술 및 관리조치 이행. 처리가 특정 목적만으로 이용되도록 하는 조치 필요	제25조
		컨트롤러가 두명 이상인 경우 합의를 통해 각자의 임무를 투명하게 결정하고 해당 합의의 내용을 정보주체에게 통보	제26조
		컨트롤러 또는 프로세서의 대리인 지정 의무	제27조
		(프로세서의 의무) 컨트롤러의 서면승인에 의해 처리(개인정보 EU 외부로 이전시 프로세서는 컨트롤러에게 해당 법률 요건 고지), EU 및 회원국 법률 준수, 개인정보처리를 승인받은 개인이 기밀유지 의무 부담하도록 할 의무, 컨트롤러의 정보처리를 지원, 처리가 종료된 후 개인정보 삭제 또는 반환, 컨트롤러의 지시가 위법한 경우 컨트롤러에게 통지. 다른 프로세서에게 위탁하는 경우 그 프로세서의 기술적 · 관리조치 보증, 행동강령 및 인증〈approved certification〉 준수	제28조
		컨트롤러, 프로세서의 권한을 대신하여 개인정보를 열람할 수 있는 개인과 프로세서는 컨트롤러의 지시에 따라서만 해당 정보를 처리	제29조
		개인정보 처리 활동 기록	제30조
		감독기관과의 협력	제31조
		적절한 기술 및 관리조치	제32조
		감독기관에 대한 개인정보 유출통지	제33조
		정보주체에 대한 개인정보 유출통지	제34조
		개인정보보호 영향평가 필수시행 요건 준수. 컨트롤러는 상업적 이익이나 공익의 보호 또는 처리의 보안을 해하지 않는 범위 내에서 적절한 범위내에서 정보주체 또는 컨트롤러의 대리인의 의견을 구해야함	제35조
		개인정보보호 영향평가에서 위험 완화조치가 없는 반면 해당 처리가 중한 위험을 초래할 것으로 예상되는 경우 처리 이전에 감독기관의 자문을 받아야 함	제36조
		개인정보보호 담당자(DPO) 지정	제37조
		개인정보보호 담당자(DPO)의 지위보장: 개인정보보호 문제에 개입할 수 있도록 보장, 전문지식을 유지하도록 지원, 독립성 보장, 업무 수행을 이유로한 해임 또는 처벌금지, DPO 업무는 최고 경영진에 직접보고	제38조
		DPO의 업무범위	제39조
		인증〈approved certification〉을 받거나, 보호조치를 통한 방법으로 EU 밖으로 개인정보를 이전하려는 컨트롤러 및 프로세서는 계약서 및 기타증서를 통해 적절한 안전조치 적용에 관련한 약정을 해야함. 인증 절차와 관련한 정보 및 관련 개인정보 처리 활동 자료를 인증기관 및 감독기관에 제공	제42조 제43조