금융기관 GDPR 이슈와 대응전략

법무법인 민후 김경환 변호사

<10가지 꼭 알아야 할 이슈와 대응방안>

1. 컨트롤러와 프로세서를 이해하라
2. 민감정보의 범위를 파악하라
3. 역내 대리인을 설치하라
4. DPO, 영향평가 의무를 이행하라
5. 행동강령, 인증 제도를 활용하라
6. 총괄 감독당국과 one-stop-shop을 파악하라
7. 이동권과 프로파일링 권리를 보장하라
8. 가명처리정보를 활용하라
9. 다양한 국외이전 제도를 활용하라
10. 과징금을 주의하라

1. 컨트롤러와 프로세서를 이해하라

o 컨트롤러

- 단독으로 또는 타인과 공동으로 개인정보 처리의 목적 및 수단을 결정하는 자연인이나 법인, 공공당국, 에이전시 또는 다른 기관
- 컨트롤러는 개인정보 처리의 목적과 수단을 결정하면 되고, 직접 개인정보를 처리하지 않아도 컨트롤러에 해당함
- 컨트롤러는 모든 처리의 수단을 결정할 필요는 없고 필수적인(essential) 처리 수단만 결정하면 됨

o 프로세서

- 컨트롤러를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공당국, 에이전시 또는 다른 기관
- 대신하여(on behalf of) : a) 컨트롤러의 이익을 위한 것이라야 하고, b) 컨트롤러의 위탁이 있어야 한다는 의미
- 프로세서는 컨트롤러와는 구별되는 법인격이어야 하며, 하나의 컨트롤러에 대하여 복수가 존재할 수 있음

o 프로세서의 책임 (제28조)

- GDPR은 95년 지침과 달리 프로세서의 의무를 규정하고 있음. 따라서 프로세서도 행정 제재나 손해배상 청구의 상대방이 될 수 있음
- 통상 컨트롤러와 프로세서가 같이 책임을 지게 됨
- 프로세서가 처리의 목적 및 수단을 결정하여 본 규칙을 위반한다면, 프로세서는 그 처리와 관련하여 컨트롤러로 간주됨

2. 민감정보의 범위를 파악하라

o GDPR의 특수한 범주의 개인정보 (제9조 제1항)

- ♦ 인종이나 민족 기원, 정치적 견해, 종교나 철학적 믿음, 노조 가입을 드러내는 개인정보
- ♦ 유전정보
- ♦ 자연인을 고유하게 식별할 수 있는 바이오인식정보
- ♦ 건강 관련 정보
- ♦ 자연인의 성생활 또는 성적취향에 관한 데이터

o 특수한 범주의 개인정보의 취급

- ♦ 원칙적으로 처리가 금지됨
- ♦ 민감정보는 '명시적' 동의 또는 법이 허용하는 경우에 프로파일링 또는 자동화된 개인 결정 가능

* 아동정보는 프로파일링 또는 자동화된 개인 결정 불가

3. 역내 대리인을 설치하라

o EU 규율의 적용범위 확대

- 역외적용 조문 (제3조)
- EU 내 정보주체에게 상품이나 서비스를 제공하는 경우 + EU 내 발생하는 정보주체 행동을 감시하는 경우

o 역외적용 실질화 제도

- 역내 대리인 지정 의무 (제4조 제17호, 제27조, 개인정보 처리가 간헐적이고, 대규모 처리가 아니며, 민감정보 등을 포함하지 않은 경우는 의무 아님)
- 대상 : EU 역외의 컨트롤러 또는 프로세서에 대한 역내 대리인
- 형식 : 서면으로 지정 의무
- 권한 : GDPR 개인정보 처리에 관련된 모든 사항
- 한계 : 역내 대리인이 지정되었다고 하여 컨트롤러 등에 대한 법적 조치가 침해되지 않아야 함

4. DPO, 영향평가 의무를 이행하라

o DPO의 지정이 의무인 경우 (제37조 제1항, 컨트롤러 및 프로세서의 지정 의무)

- ♦ 개인정보 처리가 공공당국 또는 기관에 의해 수행되는 경우 (다만 사법적 지위에 따른 법원의 경우는 예외)
- ♦ 정보주체에 대한 대규모의 정기적이고 체계적인 감시의 경우
- ♦ 민감정보나 범죄경력 및 범죄 행위에 대한 대규모의 처리

☞ 자세한 내용은 wp 248 참조

o 공동 DPO 제도 : 사업체 집단은 공동으로 1명 지정 가능

o DPO는 직원이거나 아웃소싱 가능 (제6항)

o 컨트롤러 등은 DPO를 공개하고, 감독당국에게 통지하여야 함 (제7항)

o **영향평가** : 개인정보 처리 전에 예상되는 위험 등을 평가하는 절차. 특히 새로운 기술을 사용하는 처리의 유형이 자연인의 권리와 자유에 대한 높은 위험을 초래할 것 같은 경우에 필요 (제35조 제1항)

o 의무가 되는 경우 (제3항)

☞ 자세한 내용은 'wp248' 참조

- ♦ 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
- ♦ 민감정보 또는 유죄 판결 및 형사범죄에 대한 대규모 처리를 하는 경우
- ♦ 공중이 접근 가능한 장소에 대한 대규모의 체계적인 모니터링(예 : CCTV 촬영)

5. 행동강령, 인증 제도를 활용하라

o 행동강령 (제40조 ~ 제41조)

- 특정한 산업 분야 또는 각 산업 분야의 개인정보 처리를 대표하는 그룹이 해당 산업 분야의 개인정보 처리와 관련하여 GDPR을 준수하기 위하여 마련하는 자율적 규범
- 행동강령은 정보주체 등 이해관계인과의 협의를 통해 작성하고, 감독당국의 승인을 얻어야 함

o 인증제도 (제42조~제43조)

- 목적 : 컨트롤러와 프로세서의 처리작업이 GDPR을 준수함을 입증할 목적
- 유효기간 : 3년
- 인증기관 : 인증은 소관 감독당국이나 이사회가 승인한 기준을 토대로, 소관 감독당국 또는 제43조에 언급된 인증기관에 의해 발급됨

o 행동강령과 인증은 의무 사항은 아니나, GDPR 준수 입증 요소로 중요한 역할을 함

6. 총괄 감독당국과 one-stop-shop을 파악하라

o EU 규율 체계의 단일화

- 회원국마다 상이한 개인정보보호 법령을 통일하고 일원화함
- 다만 GDPR에서 허용되는 범위 안에서 회원국의 강화 입법 보장함

o EU 규율 체계의 단일화에 따른 후속 제도 도입

- one-stop-shop 제도 (제6장)
- 총괄 감독당국 : 주된 사업장이 있는 곳의 감독당국으로서 국경간 처리에 대한 관할
- 일관성 메카니즘 (제7장 제2절)
- 유럽개인정보보호이사회(European Data Protection Board)의 신설 (제7장 제3절)

7. 이동권과 프로파일링 권리를 보장하라

o **정보이동권** (제20조)

- ♦ 정보주체가 체계화되고, 일반적으로 사용되며, 기계 판독이 가능한 형태로 제공받을 권리
- ♦ 다른 컨트롤러에게 이전할 것을 요구할 수 있는 권리

☞ 자세한 내용은 'wp242' 참조

☞ 이동권이 인정되는 경우 (제1항)

- ♦ 개인정보 처리가 정보주체의 동의에 근거하거나 계약의 이행을 위한 것인 경우
- ♦ 개인정보 처리가 자동화된 수단에 의하여 이루어지는 경우

o **처리 반대 사유** (제21조)

a) 공익이나 공적 권한 행사를 위한 목적으로 처리된 경우 또는 컨트롤러 및 제3자의 정당한 이익 추구를 위해 처리된 경우 (다만 컨트롤러가 더 중요한 정당한 근거를 입증하거나, 법적 청구권 행사 등을 위한 경우에는 처리 가능)

b) 직접 마케팅(프로파일링 포함) (처리 가능 사유 없음)

c) 과학적 또는 역사적 연구 목적 또는 통계적 목적으로 처리되는 경우 (다만 공익적 직무 수행의 경우는 처리 가능)

o **빅데이터 또는 알고리즘에 대한 권리 (제22조)**

- 인적 개입을 요구할 권리
- 정보주체가 자신의 견해를 표명할 권리
- 결정에 대한 설명을 요구하고 이의할 수 있는 권리

8. 가명처리정보를 활용하라

o 가명처리의 도입 (제4조 제5호)

- 추가정보의 이용 없이는 개인정보가 더 이상 특정 정보주체에게 귀속될 수 없는 방식으로 개인정보를 처리하는 것을 의미
- 법적취급 : 개인정보 [활용과 보호의 조화] cf) 익명정보

o 가명처리정보의 활용

a) 개인정보의 수집 목적 외의 처리와 관련해서, 개인정보를 수집한 목적 이외로 처리하기 위해서는 암호화 및 가명처리가 포함될 수 있는 적절한 보호수단을 갖추어야 한다(제6조).

b) 가명처리를 적용한 경우 data protection by design 또는 data protection by default 의무를 충족한 것으로 본다(제25조).

c) 컨트롤러와 프로세서는 가명처리 및 암호화를 통하여 적절한 보안 수준을 유지할 수 있다(제32조).

d) 공익을 위한 목적, 과학·역사 연구의 목적 또는 통계 목적에서 개인정보 처리를 할 때 정보주체의 자유와 권리를 보호하기 위하여 가명처리를 통하여 적절한 안전조치를 확보할 수 있다(제89조).

9. 다양한 국외이전 제도를 활용하라

o 개인정보의 국외 이전

- 적절성 평가에 대한 사후 감시 및 철회 근거 신설 (제45조, 적정성 결정에 근거한 이전)
- 감독당국이 채택하는 표준조항 신설 (제46조, 적절한 안전장치에 따른 이전)
- 승인된 인증이나 행동강령 신설 (제46조, 적절한 안전장치에 따른 이전)
- 소관 감독당국은 조건을 만족하는 BCR를 승인하는 과정에서 일관성 메커니즘 거쳐야 함 (제47조, 구속력 있는 기업규칙)
- 제3국의 법원 또는 행정당국의 결정에 따른 국외이전 (제48조)
- 제3자의 중대한 이익을 보호하기 위한 국외이전 (제49조, 특정상황을 위한 예외)
- 컨트롤러의 정당한 이익을 위한 국외이전 (제49조, 특정상황을 위한 예외)

10. 과징금을 주의하라

o 직전 회계년도 전세계 연간 매출액 4% 또는 2천만 유로 중 큰 금액 (사업체 집단 기준)

- ‘동의’를 비롯한 정보처리의 기본 원칙을 위반한 경우 (제5조, 제6조, 제7조 및 제9조 위반)
- 정보주체의 권리를 보장하지 않는 경우 (제12조 부터 제22조 위반)
- 제3국이나 국제기구의 수령인에게로 개인정보를 이전할 때 준수해야 할 규정을 위반한 경우 (제44조 부터 제49조 위반)

o 직전 회계년도 전세계 연간 매출액 2% 또는 1천만 유로 중 큰 금액 (사업체 집단 기준)

- 컨트롤러, 프로세서의 의무를 위반한 경우 (제8조, 제11조, 제25조 내지 제39조, 제42조, 제43조 위반)
- 인증기관의 의무를 위반한 경우 (제42조, 제43조 위반)
- 감시기관의 의무를 위반한 경우 (제41조제4항 위반)

결 어

o 개인정보 보호는 정보주체와의 신뢰를 쌓아가는 과정임

o 개인정보 보호는 기업 부담이 아닌 기업의 강점이 되어야 할 것임