대한상공회의소가 회원님께 드리는 최신 경제정보

대한상의 브리프

제41호 2017년 11월 20일

채승완 단장(한국인터넷진흥원 개인정보정책단)

편집자주 내년 5월부터 시행되는 유럽연합(EU) 개인정보보호법(GDPR)은 EU 진출 기업은 물론 EU와 관계된 모든 기업에 적용되기 때문에 국내 기업도 철저한 사전대비가 필요합니다. 이번 호에서는 GDPR의 주요 내용과 대응 방안을 소개합니다. [외부 필진 칼럼은 대한상의 견해와 다를 수 있습니다.]

기업이 알아야 할 'EU 개인정보보호법'

- 개인정보 보호하면서 기업의 활용 보장 -

지난 2016년 4월 채택되어 2년여의 유예기간을 두었던 'EU 개인정보보호법(GDPR, General Data Protection Regulation)'의 시행이 6개월 앞으로 다가왔다.

현재 유럽에 적용되고 있는 '개인정보보호지침(Directive)'은 유럽연합(EU) 회원국에게 단순히 개인정보보호의 지침만을 제시하는 성격인 반면, 2018년 5월 25일부터 새로 적용되는 GDPR은 모든 EU 회원국에 대해 직접적인 법적 구속력을 가진다.

GDPR이 국내뿐만 아니라 전 세계의 관심을 받는 또 다른 이유는 동 법의 적용 범위를 확대해 EU 역외기업들도 대상이 되도록 광범위하게 규정했고, 법의 실효성을 확보하기 위해 제재의 수준도 높였기 때문이다.

그런 만큼 그간 국내에서도 GDPR이 무엇이고 어떻게 대응해야 하는지에 대한 논의가 많았지만, 직접적인 당사자인 기업의 관심이나 구체적인 준비 노력은 아직도 미흡한 것이 현실이다.

이에 본 브리프를 통해 기업이 알아야 할 GDPR의 주요 내용과 대응전략을 소개한다.

[EU 개인정보보호의 틀 변화]

명 칭	Data Protection Directive	➡	General Data Protection Regulation
적용 시기	1995. 10. 24 ~ 2018. 5. 24	➡	2018. 5. 25 ~
입법 형식	Directive (EU 지침 제시 ▶ 회원국별로 입법)	➡	Regulation (회원국의 별도 입법절차 없이 직접 적용)
적용 범위	원칙적으로 EU에 법인을 설립한 기업에 대해서 적용	➡	EU 거주자에게 재화 · 서비스를 제공하는 EU 역외기업 포함

주요 내용 ①

소비자 권리 명확화

이번 GDPR에서는 개인정보 동의요건이 강화됐다. 즉 정보주체가 동의에 자율적이고 실질적인 결정권을 가질 수 있도록 동의 거부에 따른 불이익이 없도록 하고, 동의는 쉽게 철회할 수 있어야 하며 동의 절차는 이용약관으로부터 분리되도록 했다.

또한 침묵(silence)이나 부작위(inactivity), 디폴트 세팅(default setting) 등을 통한 수동적 동의 획득은 유효한 동의로 보지 않은 한편, 동의 조건을 읽었음을 확인하는 수준으로는 동의요건을 충족하지 못하도록 해 정보주체의 주도적이고 명시적인 의사표시를 의무화했다.

그리고 동의는 명확하고 간결하며 이해하기 쉬운 평범한 문구로 고지되어야 하며, 서비스 제공에 필요하지 않은 정보의 처리에 동의를 요구하는 것은 동의로 인정되지 않는다.

정보주체의 '정보를 제공받을 권리(Right to be informed)'를 보장하기 위해 기업이 제공해야 할 정보의 대상과 시기를 명문화했다. 정보주체로부터 직접 수집한 정보에 대해서는 수집 주체, 수집 목적, 보유 기간 등을 정보 취득 시점에 즉시 제공해야 하며, 직접 수집하지 않는 정보에 대해서는 정보 취득 후 합리적인 기간 내(최대 1개월)에 제공해야 한다.

개인정보에 대한 열람권(Right of access)과 정정권(Right to rectification)도 명문화했다. 정보주체는 개인정보의 처리가 어떻게 이루어지는지 확인하기 위해 열람을 신청하고, 개인정보가 부정확하거나 불완전하다면 정정을 요구할 권리를 부여했다. 이러한 요구가 있는 경우 기업은 개인정보 사본을 지체 없이 무상으로 제공하거나 요구 사항을 정정해야 한다.

정보주체의 삭제권(잊힐 권리, Right to be forgotten)도 새로 추가됐다. 기업은 정보주체가 개인정보의 삭제를 요구한 경우뿐 아니라, 해당 정보가 더 이상 필요하지 않은 경우나 법률 준수를 위해 삭제가 필요한 경우 등에도 해당 개인정보를 삭제해야 한다.

[개정된 EU 개인정보보호법(GDPR) 주요 내용]

소비자 권리보호	• 이해하기 쉽고 명확한 언어로 고지 및 명시적 동의 필요 • 16세 미만의 아동 정보 처리 시 법정대리인 동의 필요 • 본인에 관한 개인정보 삭제를 개인정보처리자에게 요구 가능
기업의 책임성 강화	• 개인정보 보안 침해로 피해가 예상될 경우 감독기관 및 정보주체에 통지 • 프라이버시 마크, 인증 제도 활성화 • 개인정보보호 장치의 내재화 등 자율 규제, 사전조치 강화
법 집행 및 제재	• 다수의 회원국이 관련된 소송 등의 경우 대표 감독기관이 처리 • EU 법인뿐만 아니라 EU 거주자 대상 서비스를 제공하는 경우 모두 적용 • 법 위반에 대한 벌금을 전 세계 매출액의 최대 4%까지 부과
환경 변화에 따른 조치	• 다른 서비스 제공자에게 개인정보를 이전할 권리부여 • 가명화된 정보는 동의 없이 공익, 과학적 연구 등에 활용 가능

주요 내용 ②

기업 책임 높이되 활용은 보장

기업은 GDPR 준수 입증을 위해 개인정보처리자의 책임하에 개인정보처리 활동을 문서로 기록해야 한다. 문서의 내용에는 처리의 목적, 개인정보 수령인의 범주, 보유 기간, 기술적 보안조치에 관한 내용 등이 포함되어야 한다.

또한 GDPR은 기업이 제품 개발에서 판매까지 모든 단계에 걸쳐 '개인정보보호 중심 설계(Data protection by design and data protection by default)'를 권고하고 있다.

개인정보 영향 평가(Data protection impact assessment)와 DPO(Data Protection Officer)의 지정도 중요한 이슈다. 기업은 위험도가 높은 개인정보 처리 이전에 예상되는 영향 평가를 실시해야 하고, 민감정보 처리를 핵심 활동으로 하는 경우 등에는 DPO를 의무화하고 있다.

법의 실효성 확보를 위해 제재도 강화됐다. 법을 심각하게 위반한 경우 전 세계 연간 매출액의 4% 또는 2천만 유로의 과징금이 부과될 수 있다(일반적인 위반의 경우 그 절반). 매출액 국내 상위 10대 기업의 연평균 매출이 66조 원임을 감안하면 최대 2.7조 원의 과징금이 발생할 수 있는 만큼 철저한 대비가 필요한 부분이다.

이번 GDPR 개정에는 기업의 개인정보 활용을 보장하기 위한 내용도 담겼다. 우선 정보주체가 개인정보의 이전을 요청할 수 있는 권리를 부여하여 스타트업 등 소규모 업체의 정보 접근성을 제고했다. 또한 GDPR은 기업이 정보주체에게 언제, 무엇을 알려줘야 하는지, 정보주체는 어떤 경우에 권리를 행사할 수 있는지 등을 구체적으로 규정해 기업의 정보보호와 활용에 대한 불확실성을 완화하였다.

GDPR은 개인정보 이용의 핵심인 가명화(비식별화) 개념을 명확히 하고, 개인을 알아볼 수 없도록 처리한 정보는 GDPR 적용 대상에서 제외했다. 즉, 규정대로 처리한 정보는 개인정보로 간주되지 않아 기업의 자유로운 활용이 가능해졌다.

대응 전략 ①

정확한 내용 숙지와 중요성 인지부터

앞에서 살펴본 바와 같이 GDPR의 영향은 생각보다 광범위할 것으로 예상된다. 유럽연합통계청(EuroStat)에 따르면 우리나라의 대 EU 수출 규모는 EU 교역국 평균 증가세보다 10% 이상 높은 것으로 나타났다. 향후 EU 진출을 고려하는 기업까지 포함하면 많은 기업들이 GDPR에 잠재적으로 영향을 받을 전망이다.

무엇보다 중요한 것은 GDPR이 향후 우리 기업에 미치는 영향과 중요성을 직시하는 것이다.

GDPR 및 관련 가이드라인을 명확히 숙지하는 것이 실질적인 대응의 첫 단계가 될 것이다. 시행일까지 약 6개월 정도 남은 상황에서 세부 가이드라인이 속속 발표되고 있는 만큼 해당 내용을 적시에 파악하고 기업별로 무엇을 준비할지 꼼꼼히 점검해 나가야 할 것이다.

대응 전략 ②

Global 수준으로 개인정보 관리해야

GDPR에서 도입 예정인 개인정보 영향 평가 제도의 경우 국내에서는 이미 실행되고 있을 정도로 우리나라의 개인정보보호 수준은 세계 어느 나라와 비교해도 높은 것으로 평가된다.

그만큼 우리 기업이 GDPR에 대비하기 위해 추가적으로 고민해야 할 과제는 많지 않아 보이지만 DPO(Data Protection Officer) 등 국내에서 아직 의무화되지 않은 제도에 대해서는 어떻게 도입할지 고민할 필요가 있다.

그런 만큼 국내 법과 GDPR을 포괄할 수 있는 효율적이고 체계적인 개인정보보호체계를 만드는 것이 당면한 과제다.

정부에서 기 발간한 '우리 기업을 위한 유럽 일반 개인정보보호법 안내서'나 조만간 발간될 'GDPR 대응 가이드라인' 등을 참고해 글로벌 수준의 지속 가능한 개인정보 관리 시스템을 구축해 나가야 할 것이다.

대응전략 ③

GDPR을 EU 시장 선점 기회로

GDPR 제정의 주된 이유 중 하나가 통일된 정보보호 체계를 구축해 EU를 '디지털 단일시장(Digital Single Market)'으로 만드는 것인 만큼 GDPR 시행이 EU 역내 기업은 물론 역외기업에게 줄 긍정적인 효과도 클 것으로 기대된다.

우선 그간 EU 내 국가별로 상이한 개인정보보호 규정에 대응하기 위해 소모된 비용이 크게 줄어들 것으로 예상된다. 이와 관련해 EU는 GDPR이 시행되면 모든 기업이 단일법을 적용받게 되면서 연간 총 230억 유로의 비용이 절약될 것으로 예상하고 있으며, 이에 더해 법적 확실성도 확보할 수 있을 것으로 내다봤다.

아울러 초기에 GDPR에 적극적으로 대응하는 기업의 경우 EU 시장에서의 소비자 신뢰 확보는 물론, 여타 기업이 머뭇거리는 사이 EU 시장 선점 기회까지 기대할 수 있을 것이다.

향후과제

과도한 국내 개인정보보호법 보완해야

이번 GDPR 개정을 통해 국내 기업이 처한 개인정보 활용 환경을 살펴보고 정책적인 보완과제가 무엇인지도 고민할 필요가 있다.

국내 관련 법은 '개인정보보호'가 엄격해 기업이 개인정보를 수집하고 활용하는데 제약요인이 되고 있다. 이 때문에 빅데이터를 기반으로 하는 혁신기업이 나오기 어렵다는 게 전문가들의 지적이다.

개인에 대한 정보를 가공해 특정인임을 알아볼 수 없게 처리해도 식별 가능성이 조금이라도 있으면 개인정보로 간주하는가 하면, 개인정보를 수집·이용할 때마다 건건이 사전동의를 요구하는 등의 과도한 규제가 혁신적인 사업의 출현을 막고 있다는 것이다.

개인정보는 보호하되, 기업의 개인정보 활용을 선진국 수준으로 보장해 주는 균형 있는 개인정보보호법이 마련돼야 할 것이다.

국내·외 경제지표

2017년 11월 20일 기준

1. 국내·외 경제성장률

(단위: %)

	2015	2016(E	IMF		OECD	
			2017(P	2018(P	2017(P	2018(P
한국	2.8	2.8	3.2	3.0	2.6	2.8
세계	3.4	3.2	3.6	3.7	3.5	3.6
미국	2.9	1.5	2.2	2.3	2.1	2.4
중국	6.9	6.7	6.8	6.5	6.6	6.4
일본	1.1	1.0	1.5	0.7	1.4	1.0
EU	2.0	1.8	2.1	1.9	1.8	1.8

* E : 잠정치(Estimate) / P : 예상치(Projections)

2. 환율·유가[1)]

(단위: 원(환율), 달러(유가))

	2015	2016	'17. 5월	6월	7월	8월	9월	10월
원/달러	1,131	1,161	1,125	1,130	1,134	1,131	1,132	1,132
원/엔	934	1,068	1,003	1,019	1,009	1,030	1,022	1,002
원/위안	180.1	174.4	163.5	166.1	167.5	169.2	172.3	171.1
원/유로	1,255	1,283	1,245	1,269	1,306	1,337	1,348	1,331
유가(Dubai)	32.2	53.8	50.1	46.5	50.4	49.3	55.2	58.3

3. 산업지표

(단위: %(전년동기대비))

	2015	2016	'17. 5월	6월	7월	8월	9월	10월
산업생산	1.9	3.0	2.6	1.7	2.0	2.6	7.4	-
소매판매	4.1	4.3	1.4	1.1	3.5	0.8	8.3	-
설비투자	6.9	-1.3	20.0	18.6	25.1	13.2	25.2	-
수출	-8.0	-5.9	13.1	13.4	19.5	17.3	35.0	7.1
수입	-16.9	-6.9	19.1	19.8	15.5	15.3	21.7	7.4

1) 환율은 월 평균 기준, 유가는 기말 기준