Yulchon Legal Update

2026.02.

정보통신망 침해사고 및 개인정보 유출 관련 규제 동향

1. 들어가며

최근 통신, 유통, 금융 등 분야를 막론하고 발생하고 있는 침해사고 및 대규모 개인정보 유출이 사회적으로 문제되고 있습니다. 이에 따라, 정보통신망 침해사고 및 개인정보 유출에 대한 예방과 대응을 강화하기 위하여, 국회와 정부 차원에서 법 개정 및 규제 강화가 이루어지고 있습니다.

정보통신망 침해사고에 관하여는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법")이 적용되며, 이는 과학기술정보통신부가 소관합니다. 한편, 개인정보 유출에 관하여는 개인정보 보호법이 적용되며, 이는 개인정보보호위원회가 소관합니다. 이처럼 정보통신망법과 개인정보 보호법은 별개의 법제로서 규율 대상과 소관부처를 달리하지만, 실제 해킹 사고가 발생하면 개인정보도 유출되는 경우가 많으므로 두 법률에 따른 규제가 함께 문제되는 것이 일반적입니다.

이번 제22대 국회에서는 침해사고 및 개인정보 유출사고에 관련된 다수의 정보통신망법 개정안과 개인정보 보호법 개정안이 발의되었으며, 위 개정안들의 내용을 반영한 대안들이 현재 심의 중에 있습니다. 이와 함께 과학기술정보통신부, 개인정보보호위원회 등 정부에서도 대규모 해킹사고의 예방 및 대응을 위한 업무 추진 방향을 제시하고 있습니다.

본 Legal Update에서는 현재 국회에서 심의 중에 있는 개정안의 주요 내용과 행정부에서 최근 발표한 업무 추진 방향의 주요 내용을 소개하고, 이에 따른 기업의 역할과 대응방안에 관하여 안내해 드립니다.

2. 법 개정 및 규제 강화의 주요 내용

현재 국회에서 심의중인 정보통신망법 개정안 및 개인정보 보호법 개정안의 주요 내용은 다음과 같습니다. 아래 법률안들은 국회 본회의를 통과하면 정부로 이송되어 공포되며, 공포 후 6개월이 경과한 날부터 시행됩니다. 다만, 정보보호수준 평가는 공포 후 1년이 경과한 날부터 시행하고, ISMS-P 의무화는 2027. 7. 1.부터 시행되도록 하여 시행 시점을 유예하고 있습니다. 개정안들은 주로 (1) 정보보호 거버넌스 개선 및 관리체계 강화에 관한 내용과 (2) 사고 발생시 조사 및 제재에 관한 내용을 담고 있습니다.

Related Areas

IP & Technology 융합

빅데이터 & 인공지능

개인정보보호

Contact

김선희 변호사
02-528-5838
kimsh@yulchon.com

김나래 전문위원
02-528-5734
nrkim@yulchon.com

배상호 고문
02-528-6110
shbae@yulchon.com

최승혁 변호사
02-528-6156
synghyokchoi@yulchon.com

구분	정보통신망법 개정안	개인정보 보호법 개정안
거버넌스 개선 및 관리체계 강화	• 정보보호 최고책임자(CISO)의 업무에 ①정보보호에 필요한 인력 관리 및 예산 편성, ②이사회에 대한 정보보호 현황 보고가 추가됨 • 일정 규모 이상 정보통신서비스 제공자에 대하여 정보보호위원회 설치의무 부과 • 일정 규모 이상 사업자를 대상으로 매년 정보보호수준 평가 시행 • 정보 처리 규모와 사회적 파급력을 고려하여 ISMS 인증기준 및 절차를 강화하여 적용	• 사업주 또는 대표자를 개인정보 처리 및 보호에 관한 최종책임자로 규정하고, 개인정보 보호책임자(CPO)의 업무에 ① 개인정보 보호에 필요한 인력 관리 및 예산 확보, ②대표자 및 이사회에 대한 개인정보 보호 현황 보고가 추가됨 • 일정 규모 이상 개인정보처리자에 대하여 ① 개인정보 보호책임자(CPO) 임면 시 이사회 의결을 거치도록 하고, ② 개인정보보호위원회에 CPO 지정에 관한 사항을 신고하도록 함 • 일정 규모 이상 개인정보처리자에 대하여 ISMS-P 인증 의무화
사고 발생에 대한 대응 및 제재	• 침해사고 발생 사실을 알게 된 때로부터 24시간 이내에 이용자에게 통지할 의무 신설 • 과학기술정보통신부 산하의 침해사고조사심의 위원회가 침해사고 발생 여부에 대한 조사가 필요하다고 인정하는 경우에는 과학기술정보통신부가 침해사고 발생 여부 및 원인을 조사하고 해당 정보통신서비스 제공자에게 필요한 조치를 명할 수 있음 • 시정명령 불이행, 자료 제출 거부, 거짓 제출, 조사 방해 등의 경우 이행강제금 부과(1일 평균 매출액의 0.03% 이내) • 고의 또는 중과실에 의하여 침해사고가 5년 이내에 반복하여 발생한 경우 연간 매출액의 3% 이하의 과징금 부과 • 침해사고 관리·대응 매뉴얼 작성의무 부과	• 개인정보 분실, 도난, 유출뿐만 아니라 위변조, 훼손까지 정보주체 통지 및 개인정보위 신고 대상에 포함됨(이하 "유출등"). • 정보주체에게 미치는 영향과 위험 정도가 큰 유출등(대통령령으로 정할 예정)의 경우 개인정보 유출등 가능성이 있음을 알게 된 때에 지체 없이 관련된 모든 정보주체에게 통지하여야 함 • 정보주체에 대한 통지 항목에 정보주체의 법적 권리와 행사 방법에 관한 정보 추가 • ①고의 또는 중과실로 과징금을 부과받은 자가 3년 이내에 같은 유형의 위반행위를 반복하거나, ② 고의 또는 중과실로 과징금 대상 위반행위를 하여 피해 규모가 1천만 명 이상이거나, ③ 개인정보위 시정명령 미이행으로 인하여 개인정보가 유출등 된 경우 과징금 강화(전체 매출액의 10% 이내). 한편, 개인정보 보호를 위한 예산, 인력, 설비, 장치 등의 투자 및 운영 등 사유(대통령령으로 정할 예정)가 있는 경우에는 과징금을 감경함.

한편, 과학기술정보통신부는 2026년 업무계획에 주요 쟁점이슈로 '민간 분야 해킹사고 대응'에 관한 사항을 포함하였습니다. 또한, 개인정보보호위원회도 2026년 개인정보 중점 조사 분야, 조사 제도 및 절차 개선에 관한 사항 등 조사업무 추진 방향을 공개하였습니다. 두 부처가 공개한 주요 내용은 다음과 같습니다.

과기정통부	개인정보보호위원회
• 침해사고에 관한 신속한 조사 및 투명한 결과 공개 • 법 위반 사항에 대한 엄정 조치 • 해킹 정황이 발생한 경우 직권조사 • 제재조치 강화(반복 사고기업에 대한 과징금 신설, 재발방지 미이행시 이행강제금 부과 등)	• 중점 조사 분야 - 대규모 개인정보처리자 중 사고 빈도, 서비스 성격, 민감도 등을 고려하여 우선 점검 대상자 선정 - 생체·영상정보 등 고위험 개인정보 처리에 대한 집중 점검 - 주요 웹·앱 서비스 모니터링을 통해 이용자 선택 왜곡 등 다크패턴을 집중 점검 - 엔터테인먼트 업계의 개인정보 실태점검 및 개선 조치(공연장에서 아동·청소년 개인정보 과도한 수집 등) - AI 채용솔루션 및 이용기관을 대상으로 자동화된 결정 해당 여부, 투명성 확보 노력 점검 - 주요 공공시스템에 대한 취약점 점검 의무 강화 및 보완 대책 수립 - 기업결합(M&A) 및 도산(파산·회생) 시 수반되는 이용자 개인정보 이전·파기의 적법성·안전성 관련 집중 점검 • 조사 제도 및 프로세스 개선 - 침해신고센터 기능 강화 - 자료제출명령 미이행에 대한 이행강제금, 증거보전 명령 도입 - 대규모 개인정보처리자에 대한 실태점검 정례화 - 과징금 부과기준 강화 - 선제적 대규모 예방투자 기준 마련 - 시정명령 범위를 예방 조치 사항으로 확장 - 시정명령 불이행 시 이행강제금 도입

3. 기업의 역할과 대응방안

위에서 살펴본 바와 같이, 국회와 정부는 기업들의 정보보호 사고 예방을 위한 사전적 조치를 유도하면서 정보보호 거버넌스 강화를 요구하고 있습니다. 이러한 규제 환경 변화에 따라, 기업은 아래와 같은 사항을 중심으로 대응할 필요가 있습니다.

- **우선, 각 기업에 적용되는 규제 수준을 정확히 파악하고, 해당 규제 수준에 맞는 정보보호 현황을 점검할 필요가 있습니다**. 개정법안들은 기업의 매출 규모, 서비스의 성격, 처리하는 개인정보의 유형과 규모, 사회적 파급력 등에 따라 규제 수준을 차등하여 적용할 것을 예정하고 있습니다.

- **정보보호 거버넌스에 대한 전반적인 점검 및 개선이 필요합니다**. 개정법안들은 CISO와 CPO의 업무 범위와 권한을 확대하는 한편, 대표자의 책임을 명시하는 등 거버넌스 강화를 요구하고 있습니다. 이에 따라 현재 기업의 정보보호 거버넌스 체계가 강화된 법령상 요구 수준에 부합하는지, CISO와 CPO의 책임과 권한이 법령에 따라 명확히 설정되어 있는지 점검할 필요가 있습니다.

- **정보보호 분야의 인력 및 조직에 대한 투자와 강화 필요성이 커지고 있습니다**. 개정법안들은 정보보호수준 평가의 정례화, ISMS-P 인증 의무화, 침해사고 관리·대응 매뉴얼 작성 의무 등 사전 규제를 강화하는 한편, CISO 및 CPO로 하여금 정보보호에 필요한 인력 관리 및 예산 편성 권한과 책임을 부여하고 있습니다. 이에 따라 일정 규모 이상의 정보보호 조직을 상시적으로 운영하는 체계를 갖출 필요가 있습니다.

한편, 사전적 예방 조치에 못지 않게, 침해사고 및 개인정보 유출 사고가 발생한 경우 신속하고 적절하게 대응하기 위한 체계를 갖출 필요성도 커지고 있습니다.

- **기업의 사고 대응 체계를 전반적으로 점검하고, 법령에서 요구하는 수준에 맞게 정비할 필요가 있습니다**. 개정법안은 기업으로 하여금 침해사고 관리·대응 매뉴얼을 작성할 의무를 부과하는 한편, 이용자 및 정보주체에 대한 통지의무 범위를 확대하는 등 사고 대응 관련 규제를 강화하고 있습니다. 이에 따라 기존 사고 대응 절차, 내부 보고 체계 및 통지 프로세스 등이 강화된 요건에 부합하는지 선제적으로 점검하고 필요한 개선 조치를 마련할 필요가 있습니다.

- **규제기관의 자료 제출 요구, 시정명령 등에 대하여 신속한 대응 체계를 갖추는 것이 중요합니다**. 개정법안은 규제기관의 시정명령을 이행하지 않거나 자료 제출을 거부하는 행위에 대한 제재를 강화하고 있으며, 관련 규제기관도 조사의 실효성 확보를 위하여 제재 규정을 엄격하게 적용하겠다는 입장입니다. 이에 따라 기업은 규제기관의 요구에 신속하고 적절하게 대응할 수 있도록 내부 의사결정 절차와 대응 프로세스를 정비할 필요성이 있으며, 필요할 경우 규제기관 대응을 위한 별도 조직 또는 TF를 구성하는 것을 고려해 볼 수 있습니다.

- **사고 재발 방지를 위한 사후 관리 체계를 수립할 필요가 있습니다**. 개정법안은 반복적 사고 발생에 대한 제재를 강화하고 있으므로, 동일한 유형의 사고가 반복되지 않도록 사고 원인 및 개선사항을 파악하고 이를 정보보호 관리체계에 반영하여 관리할 필요가 있습니다.

법무법인(유) 율촌은 거버넌스 개선, 사전 규제 검토, ISMS-P 인증 취득, 침해 개인정보 유출 사고 대응 등 정보보호 규제 전반에 걸친 풍부한 자문 경험을 바탕으로, 변화하는 규제 환경 속에서 기업이 선제적으로 대응할 수 있도록 전략적 지원을 제공하겠습니다.