

October 8, 2026

개정 정보통신망법 및 시행령 시행: 정보보호·침해사고 대응 및 불법스팸 규제 강화

I. 개정 정보통신망법 및 시행령 시행

2026년 3월 12일 국회 본회의를 통과한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 개정법은 2026년 3월 31일 공포되었고, 2026년 10월 1일부터 시행되고 있습니다. 이에 따른 후속 조치로 대통령령 제36735호 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부개정령」(이하 “시행령”)도 2026년 9월 30일 공포되어 2026년 10월 1일부터 시행되었습니다.

지난 3월 뉴스레터에서는 개정법이 도입한 정보보호 최고책임자(CISO)의 권한·책임 확대, 정보보호위원회 설치, 침해사고 통지·조사, 이행강제금 및 과징금, 불법스팸 규제 강화 등 입법의 주요 골자를 소개하였습니다. 이번에 공포된 시행령은 이러한 제도의 적용 대상과 운영 방식, 이용자 통지 기준, 과징금·이행강제금 산정기준 등을 구체화하였으므로, 이제 기업은 개정법의 방향뿐 아니라 확정된 세부 기준을 전제로 실제 내부 체계와 사고 대응 절차를 점검할 필요가 있습니다.

II. 주요내용

구분	시행령 주요내용
CISO·정보보호위원회	CISO 자격요건과 추가 업무를 구체화하고, 일정 사업자에 정보보호위원회 설치·연 1회 이상 개최 및 최고경영자·이사회 보고 체계를 마련
ISMS 차등 적용	강화된 정보보호 관리체계 인증의 적용 대상을 매출액, 사업 유형 및 최근 침해사고 이력 등에 따라 구체화하고 서면·현장심사를 병행
침해사고 통지·대응	2시간 이상 서비스 장애, 이용자 정보 침해 등의 경우 이용자에게 지체 없이 통지하도록 하고 통지 내용·방법과 후속 통지 절차를 규정
매뉴얼·피해구제	일정 사업자에게 침해사고 관리·대응 매뉴얼 작성·제출 의무를 부과하고, 피해구제 조치 결과를 신고 후 14일 이내 제출하도록 구체화
제재·불법스팸	이행강제금 및 반복 침해사고 과징금의 구체적 산정기준을 마련하고, 광고성 정보 전송 위반에 대한 제한조치 및 과징금 기준을 세분화

1. CISO 자격·업무 및 정보보호위원회 운영 기준 구체화

개정법은 정보통신서비스 제공자의 정보보호 최고책임자(CISO)를 **임원**으로 지정하도록 하면서 정보보호 관련 인력 관리, 예산 편성 및 이사회 보고 등 권한과 책임을 강화하였습니다. 시행령은 CISO의 자격을 사업주·대표자, 이사·업무집행자·업무집행사원, 사실상 이사 또는 집행임원 등으로 구체화하였고, 중소기업기본법상 중소기업 중 전기통신사업자, 정보보호 관리체계 인증을 받아야 하는 자, 개인정보처리자 및 통신판매업자의 경우 정보보호 관련 업무를 총괄하는 부서의 장도 CISO로 지정할 수 있도록 하였습니다.

또한 CISO의 업무에는 정보통신시스템 또는 정보통신서비스의 도입·개시·변경 시 보안성 검토와, 정보통신시스템 구축·운영·관리 또는 정보처리 업무 수탁자 및 클라우드컴퓨팅서비스 제공자에 대한 정기적인 보안수준 점검·감독이 포함됩니다. 공급망과 클라우드 이용에 대한 보안 검토가 CISO의 법정 업무 범위에 명시되었다는 점에 유의할 필요가 있습니다(시행령 제36조의7제7항).

정보보호위원회 설치 대상은 시행령 제36조의7제1항제2호부터 제4호까지의 정보통신서비스 제공자로 구체화되었습니다. 위원회는 CISO를 위원장으로 하여 정보보호, 개인정보 처리, 전산 운영·개발, 준법·법무, 재무, 인사 관련 부서의 장 등을 중심으로 구성하고, 매년 1회 이상 정기적으로 개최하여야 합니다. 심의 결과는 최고경영자에게 보고하여야 하며, 정보보호에 중대한 영향을 미치는 사항은 이사회에도 보고하여야 합니다(시행령 제36조의10 및 제36조의11).

2. 정보보호 관리체계(ISMS) 인증의 강화 적용 대상 확정

시행령은 ISMS 인증심사에 서면심사와 현장심사를 병행하도록 하는 한편, 정보의 규모와 사회적 파급력 등을 고려하여 강화된 인증 기준·절차를 적용할 대상을 구체화하였습니다. 강화 적용 대상은 다음과 같습니다(시행령 제55조의7제3항).

- 전 사업연도 매출액이 1 조원 이상인 자 중 주요정보통신서비스 제공자 또는 집적 정보통신시설 사업자
- 전 사업연도 매출액이 3 조원 이상인 정보통신서비스 제공자
- 최근 3 년 이내 침해사고가 발생하여 민·관합동조사단의 조사를 받았거나 반복 침해사고에 따른 과징금을 부과받은 정보통신서비스 제공자

아울러 반복 침해사고에 대한 과징금을 부과받은 경우 중 침해사고의 중대성이 “매우 중대한 침해사고” 또는 “중대한 침해사고”에 해당하는 경우 등은 ISMS 인증 취소

사유가 될 수 있도록 규정되어 있어, 침해사고 제재가 인증 유지에도 직접적인 영향을 미칠 수 있습니다(시행령 제52조의2).

3. 이용자에 대한 침해사고 통지 기준 및 조사 절차 구체화

개정법은 일정한 침해사고가 발생한 경우 이용자에게 지체 없이 통지하도록 하였고, 시행령은 그 대상과 통지 방법을 구체화하였습니다. 이용자 통지 대상에는 다음의 침해사고가 포함됩니다(시행령 제58조의9).

- 정보통신서비스 장애 또는 기능 중단 상태가 2 시간 이상 지속된 침해사고
- 이용자 정보가 분실·도난·유출·변조·훼손·유용되었거나 그러할 가능성이 있는 침해사고
- 이에 준하는 경우로서 이용자 정보보호에 중대한 영향을 미칠 우려가 있는 침해사고

통지에는 (i) 사고 발생 일시, 원인·피해내용, (ii) 침해사고에 대한 조치사항 등 대응 현황, (iii) 침해사고로 발생할 수 있는 피해를 최소화하기 위한 이용자의 대처방법에 관한 정보, (iv) 이용자 피해구제 조치의 내용, (v) 피해구제 관련 민원 처리 담당부서 및 연락처가 포함되어야 합니다. 사고 원인이나 피해내용이 아직 구체적으로 확인되지 않은 경우에는 침해사고가 발생한 사실, 그때까지 확인된 내용과 위 (ii)부터 (v)까지의 을 먼저 통지한 후 추가로 확인하는 내용에 대해서는 확인하는 즉시 통지하여야 합니다. 통지는 서면, 전화, 전자우편, 팩스, 문자전송 등으로 할 수 있고, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 홈페이지에 30일 이상 게시하는 방식으로 갈음할 수 있습니다.

한편, 침해사고조사심의위원회는 위원장을 포함하여 15명 이내의 위원으로 성별을 고려하여 구성되며, 침해사고 발생 여부에 대한 조사가 필요한 경우 조사 범위·방식 등을 심의합니다. 이에 따라 침해사고가 이미 확정된 경우뿐 아니라 발생이 의심되는 단계에서도 조사 필요성에 대한 심의를 거쳐 규제기관의 조사와 피해 확산 방지 조치가 이루어질 수 있다는 점을 고려하여야 합니다(시행령 제58조의2 및 제58조의3).

4. 침해사고 관리·대응 매뉴얼 및 이용자 피해구제 의무 구체화

침해사고 관리·대응 매뉴얼 작성·제출 의무는 ① 직전 사업연도 말 기준 자산총액이 5 조 원 이상인 정보통신서비스 제공자, ② 정보보호 관리체계(ISMS) 의무인증 대상자 중 직전 사업연도 말 기준 자산총액이 5 천억 원 이상인 정보통신서비스 제공자, ③

중기업 중 전기통신사업자, ISMS 의무인증 대상자, 개인정보 처리방침 공개 대상 개인정보처리자 또는 통신판매업자에 해당하는 정보통신서비스 제공자 및 ④ 그 밖에 자본금 1 억 원 이하 사업자, 소기업, 또는 앞서 열거한 전기통신사업자·ISMS 의무인증 대상자·개인정보 처리방침 공개 대상 개인정보처리자·통신판매업자에 해당하지 않는 중기업을 제외한 정보통신서비스 제공자에게 적용됩니다. 이들 사업자는 침해사고의 예방 및 사고 발생 시 신속한 대응을 위한 관리·대응 매뉴얼(이하 “매뉴얼”)을 작성하여 과학기술정보통신부장관에게 제출하여야 합니다. 매뉴얼에는 ① 침해사고 예방 및 피해 확산 방지를 위한 조직체계·담당자·정보공유 방법, ② 침해사고 발생 시 피해 최소화를 위한 이용자 피해구제 조치사항, ③ 침해사고 예방을 위한 점검·대응 체계, ④ 매뉴얼의 정기적 점검·현행화 방안, ⑤ 그 밖에 매뉴얼 작성·운용 실태 점검의 효율성과 전문성을 높이기 위해 과학기술정보통신부장관이 필요하다고 인정하는 사항이 포함되어야 합니다. 과학기술정보통신부장관은 정보보호 공시 이행 여부, 최근 침해사고 이력, 서비스 이용자 수 등을 고려하여 서면조사 또는 현장조사 방식으로 매뉴얼의 작성·운용 실태를 점검할 수 있습니다. 과학기술정보통신부장관은 매뉴얼 작성·운용 실태점검을 하는 경우 점검의 목적, 대상, 방법, 기간 등을 점검 시작 7 일 전까지 해당 매뉴얼 작성의무자에게 서면으로 통보해야 하며, 다만, 침해사고가 발생하는 등 긴급히 점검할 필요가 있는 경우에는 매뉴얼 작성·운용 실태점검의 개시와 동시에 서면을 제시하거나 구두로 통지할 수 있습니다. (시행령 제 60 조의 15).

또한 침해사고로 인한 이용자 피해구제와 관련하여, 정보통신서비스 제공자는 피해구제 조치의 내용, 대상·범위 및 결과 등을 침해사고 신고일부터 14일 이내에 과학기술정보통신부장관에게 제출하여야 합니다. 부득이한 사유가 인정되는 경우에는 14일을 넘지 않는 범위에서 한 차례 연장할 수 있습니다(시행령 제60조의16).

5. 이행강제금 및 반복 침해사고 과징금의 산정기준 확정

조사 과정에서의 자료 미제출·허위 제출, 현장조사 방해 또는 시정명령 불이행 등에 대한 재명령을 이행하지 않는 경우 부과되는 이행강제금은 시행령상 1일 평균매출액의 1만분의 2(0.02%)를 1일당 기준금액으로 하며, 명령 이행 노력과 불이행 정도 등을 고려하여 2분의 1 범위에서 가중·감경할 수 있습니다. 다만 법률이 정한 상한을 초과할 수 없습니다. 재명령의 이행기간 종료일부터 90일이 지난 후에도 이행하지 않는 경우에는 그 이후 매 90일마다 추가로 부과·징수할 수 있습니다(시행령 제60조의10 및 별표 5의2).

정보통신서비스 제공자의 고의 또는 중과실로 5년 이내 2회 이상 침해사고가 발생한 경우의 과징금은 최근 침해사고 발생일이 속하는 사업연도를 기준으로 산정한

매출액에서 침해사고와 관련이 없는 매출액을 제외한 금액을 기초로 산정합니다. 시행령은 침해사고의 중대성에 따라 부과기준율을 “매우 중대한 침해사고” 2.1% 이상 2.7% 이하, “중대한 침해사고” 1.5% 이상 2.1% 미만, “보통 침해사고” 0.9% 이상 1.5% 미만, “약한 침해사고” 0.03% 이상 0.9% 미만으로 구분하였습니다. 이후 조사 협조, 피해 회복·확산 방지, 정보보호 인력·예산과 위원회 운영, 매뉴얼 작성 등 정보보호 노력 등을 반영하여 가중·감경하되 법률상 상한을 초과할 수 없습니다(시행령 제60조의11 및 별표 5의3).

6. 불법스팸 관련 제한조치 및 과징금 기준 구체화

시행령은 정보통신서비스가 불법 광고성 정보 전송에 이용되는 경우 서비스 제공자가 취하여야 할 조치와 과징금 산정기준을 구체화하였습니다.

정보통신서비스 제공자는 자신의 서비스가 위법한 광고성 정보 전송에 이용되는 것을 인지한 경우 즉시 해당 광고성 정보 전송을 중단하고, 보안체계 취약점이 원인인 경우 이를 점검·개선하며, 이용계약·약관의 미비점이 원인인 경우 관련 내용을 개선하고 재발 방지 계획을 수립·점검하여야 합니다(시행령 별표 6의2). 과징금의 경우 위반행위와 관련 없는 매출액을 제외한 매출액을 기준으로 하며, 일반적인 광고성 정보 전송 규정 위반은 중대성에 따라 1% 이상 4% 이하의 부과기준율이, 광고성 정보 전송 시 금지된 행위¹를 하는 경우(법 제50조제5항 위반) 및 불법행위를 위한 광고성 정보를 전송하는 경우(제50조의8 위반)에는 3% 이상 6% 이하의 부과기준율이 적용됩니다(시행령 제64조의2 및 별표 6의3).

III. 시행시기 및 경과조치

개정 정보통신망법과 이번 시행령은 2026년 10월 1일부터 이미 시행 중입니다. 따라서 위 의무의 적용 대상인 사업자는 더 이상 시행 준비 단계가 아니라 실제 법 준수 단계에 있다는 점에 유의할 필요가 있습니다.

다만 정보보호 수준에 대한 정기적 평가 제도(법 제45조의5)와 관련 과태료 규정은 공포 후 1년이 경과한 날부터 시행되므로 2027년 4월 1일부터 적용될 예정입니다. 시행령 역시 정보보호 수준 평가 관련 자료제출 거부·거짓 제출에 대한 과태료 기준을

1 ①광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 행위, ②숫자·부호 또는 문자를 조합하여 전화번호·전자우편주소 등 수신자의 연락처를 자동으로 만들어 내는 행위, ③영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 행위, ④ 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 행위, ⑤영리목적의 광고성 정보를 전송할 목적으로 수신자를 기망하여 회신을 유도하는 각종 행위

2027년 4월 1일부터 시행하도록 정하고 있습니다.

또한 시행 당시 종전 규정에 따라 정보보호 관련 업무를 총괄하는 부서의 장을 CISO로 지정·신고한 사업자 중 시행령 제36조의7제1항제4호에 해당하는 경우에는 시행일부터 6개월 이내에 새 자격요건에 맞는 CISO를 다시 지정·신고하여야 합니다.

IV. 시사점

이번 정보통신망법 시행에 따라 기업들은 법령을 준수할 수 있도록 다음의 사항을 점검할 필요가 있습니다.

- CISO의 현 직위가 개정 시행령상 자격요건을 충족하는지 확인하고, 정보보호위원회의 구성원·운영규정·연간 개최 일정 및 최고경영자·이사회 보고 절차를 정비
- 매출액·사업유형·최근 3년 침해사고 이력을 기준으로 강화된 ISMS 적용 여부를 판단하고, 서면심사와 현장심사를 함께 고려한 인증 대응 체계를 준비
- 2시간 이상 서비스 장애 및 이용자 정보 침해 가능성을 포함한 이용자 통지 트리거를 사고대응 매뉴얼에 반영하고, 최초 통지·후속 통지·홈페이지 공지 절차를 구체화
- 침해사고 관리·대응 매뉴얼에 시행령상 필수 항목을 반영하고 정기 점검·현행화 기록, 피해구제 조치 및 신고 후 14일 내 제출 자료를 사전에 표준화
- 이행강제금·과징금 산정에 필요한 매출액 자료를 구분 관리하고, 조사 협조·피해 확산 방지·정보보호 투자 등 감경 요소를 입증할 수 있는 내부 기록을 체계적으로 축적
- 광고성 정보 전송을 외부 사업자에게 위탁하는 경우 전송자격인증 여부를 확인하고, 계약·약관과 서비스 차단·복구 프로세스를 시행령상 제한조치 기준에 맞추어 점검

* * *

법무법인(유한) 태평양은 정보통신망법상 CISO 및 정보보호위원회 체계 정비, ISMS 적용 대상 검토, 침해사고 대응 매뉴얼 및 이용자 통지·피해구제 프로세스 구축, 규제기관 조사 대응, 이행강제금·과징금 및 불법스팸 규제 대응과 관련하여 다양한 자문 경험을 보유하고 있습니다. 개정법 및 시행령의 적용과 관련하여 문의사항이 있으시면 언제든지 연락하여 주시기 바랍니다.

관련 구성원

박지연

변호사

T 02.3404.0655

E jiyeon.park@bkl.co.kr

강태욱

변호사

T 02.3404.0485

E taeuk.kang@bkl.co.kr

윤주호

변호사

T 02.3404.6542

E juho.yoon@bkl.co.kr

이강혜

변호사

T 02.3404.7454

E kanghye.lee@bkl.co.kr

법무법인(유한) 태평양의 뉴스레터에 게재된 내용 및 의견은 일반적인 정보제공만을 목적으로 발행된 것이며, 법무법인(유한) 태평양의 공식적인 견해나 어떤 구체적 사안에 대한 법률적 의견을 드리는 것이 아님을 알려드립니다. 뉴스레터와 관련된 문의사항이 있을 경우 위 연락처로 문의주시기 바랍니다.