제428국회(임시회)
제2차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

<개인정보 불법유통 정황 모니터링 및
개인정보 유출사실 개별 통지 의무화 등>

▣ 이정문의원 대표발의(의안번호 제2210294호)
▣ 이해민의원 대표발의(의안번호 제2210762호)
▣ 이헌승의원 대표발의(의안번호 제2210795호)
▣ 최민희의원 대표발의(의안번호 제2210936호)

2025. 8.

정 무 위 원 회

수석전문위원 정명호

목 차

Ⅰ. 제안경위 ····· 1

Ⅱ. 제안이유 및 주요내용 ····· 2

Ⅲ. 검토의견 ····· 6

1. 총괄 ····· 6

2. 개인정보처리자의 불법유통 개인정보 모니터링 및 고발 의무화 등 (이정문의원안) ····· 13

3. 정보주체의 불법유통 개인정보 신고(이정문의원안) ····· 25

4. 개인정보 유출 통지 내용 구체화 및 유출사실 개별 통지 의무화 (이해민의원안·최민희의원안) ····· 28

5. 개인정보 유출 신고기한 단축(이헌승의원안) ····· 37

6. 개인정보 유출 시 후속조치 수립·통지 의무화(이해민의원안) ····· 41

Ⅰ. 제안경위

1. 이정문의원안

가. 제 안 자 : 이정문의원 등 10인

나. 제 안 일 : 2025. 5. 1

다. 회 부 일 : 2025. 5. 2

2. 이해민의원안

가. 제 안 자 : 이해민의원 등 12인

나. 제 안 일 : 2025. 6. 12

다. 회 부 일 : 2025. 6. 13

3. 이헌승의원안

가. 제 안 자 : 이헌승의원 등 13인

나. 제 안 일 : 2025. 6. 13

다. 회 부 일 : 2025. 6. 16

4. 최민희의원안

가. 제 안 자 : 최민희의원 등 12인

나. 제 안 일 : 2025. 6. 19

다. 회 부 일 : 2025. 6. 20

Ⅱ. 제안이유 및 주요내용

1. 이정문의원안

현행법은 개인정보의 안전한 관리를 위한 보호조치 기준을 정하고 있으나 개인정보 유출사고가 지속적으로 발생하고 있으며 그 피해는 국민 개개인의 일상생활과 재산권에 심각한 영향을 미치고 있음.

특히 2025년 4월 22일, 2500만 명의 가입자를 보유한 SK텔레콤의 대규모 USIM 정보 유출 사고 발생 사례와 같이 대규모 개인정보를 수집하는 기업의 사고가 반복적으로 발생하고 유출된 개인정보가 불법거래 사이트를 통해 유통되면서 2차 피해로 이어지는 사례가 빈번함에도 불구하고 유출 당사자인 개인정보처리자가 사후적으로 유통 실태를 추적하고 확산을 방지하는 노력이 미흡하다는 지적이 있음.

이에 일정 건수 이상의 개인정보 유출사고가 발생한 경우 등 개인정보가 유출된 경우 일정 기간 동안 불법거래 사이트 등을 모니터링하고 유출 정보의 고발 등 후속 조치를 수행하도록 하여 개인정보처리자의 정보보호 책임을 강화하고 실질적인 피해자 보호방안을 도입하려는 것임(안 제34조의3 신설 등).

2. 이해민의원안

최근 SKT 내부망이 해커의 공격을 받아 가입자 정보가 외부로 유출되는 보안 사고가 발생했음. 이는 대규모 피해로 이어질 수 있는 중대한 침해사고임에도 불구하고, 정보 주체인 이용자는 이 사실을 신속하고 충분하게 전달받지 못함. 사고 발생 후 4일이 지나서 회사 홈페이지 공지가 올라왔고, 개별 문자 안내는 5일이 지난 시점부터 이루어졌음. 통지 내용이 구체적이지 않아, 이용자가 사태의 심각성이나 향후 예상되는 위험 및 필요한 대응 방안을 제대로 인지할 수 없었음.

이처럼 침해사고 자체뿐 아니라, 사고 발생 이후 미흡한 후속 조치가 소비자 불안과 사회 혼란을 더욱 증폭시킨다는 지적이 있음.

이에 유출 항목에 대한 통지 내용을 구체화하고, 개별 통지를 의무화하고자 함. 또한 개인정보처리자가 사고 발생 후 후속 조치 계획을 수립하여 개인정보보호위원회 및 정보 주체에게 이를 알리도록 함으로써, 사고 수습과 재발 방지 체계에 대한 책임성을 강화하고자 함(안 제34조).

3. 이헌승의원안

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 해킹·악성코드 등으로 인한 보안침해 사고 발생 시 24시간 이내에 관계 기관에 신고하도록 의무를 규정하고 있는 반면, 현행법령은 개인정보 유출 등의 사고가 일어난 경우 그 유출을 인지한 때로부터 72시간 이내에 신고하도록 정하여 제도상 신고 기한의 불일치가 발생하고 있음.

이로 인해 운영 주체가 동일하거나 유사한 사고에 대하여 서로 다른 신고 기준을 적용받게 되어, 현장 혼선과 불필요한 행정 부담이 가중될 우려가 있음.

또한, 현행법은 대통령령에서 정하고 있는 신고기한인 72시간을 초과하여 신고하는 경우에 대한 명확한 제재 규정이 없어 신고 의무를 실효성 있게 담보하기 어렵다는 지적이 있음.

이에 개인정보 유출·침해 사고를 인지한 때로부터 24시간 이내에 관계 기관에 신고하도록 의무를 강화하고, 이행하지 아니할 경우 과태료를 부과할 수 있도록 하여 법체계의 일관성을 확보하고, 개인정보 처리자의 책임 의식을 제고하여 국민의 개인정보 보호 수준을 실질적으로 강화하려는 것임(안 제34조제3항).

4. 최민희의원안

현행법은 개인정보 유출 시 유출된 항목, 시점, 대응 조치 등 법정사항을 정보주체에게 개별적으로 통지하도록 정하면서 예외적인 경우 홈페이지 공지로 이를 갈음할 수 있도록 하고 있음.

그러나, 개인정보처리자가 유출 사고에도 불구하고 법정 사항에 대한 개별적 통지 없이 홈페이지에 간략한 안내만을 게시한 것은 본인의 개인정보 유출 여부를 신속히 파악하기 어렵게 하고, 적절한 대응조치를 취할 기회를 놓치게 만들어 추가적인 유출 위험에 취약하다는 지적이 있음.

이에 유출된 개인정보의 정보주체를 특정할 수 없고, 유출 규모가 대통령령으로 정한 기준 이상일 경우에는 유출등이 확인된 정보주체 및 유출의 가능성이 있는 모든 정보주체에게 법정 통지사항을 개별적으로 통지할 것을 의무화하여 정보주체의 권리보호를 강화하고, 개인정보처리자의 책임 있는 대응을 유도하려는 것임(안 제34조제2항 신설 등).

Ⅲ. 검토의견

1. 총괄

□ 2025년 4월 18일 23시 20분, SK텔레콤(이하 “SKT라 함”)은 평소 대비 대용량 데이터가 외부로 전송된 정황을 인지하고 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”이라 함)」에 근거하여 4월 20일 한국인터넷진흥원에 침해사고를 신고[1]하였음.

○ 과학기술정보통신부는 SKT의 유심정보 유출을 중대한 침해사

---

1) 「정보통신망법」상 사고인지 시점부터 24시간 이내에 신고를 해야 하며, 이를 위반 시 3천만원 이하 과태료 부과 대상 → SKT는 침해사고 인지 후 24시간이 도과하여 신고하였으므로 「정보통신망법」상 과태료 부과 예정

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.
② 과학기술정보통신부장관이나 한국인터넷진흥원은 제1항에 따라 침해사고의 신고를 받거나 침해사고를 알게 되면 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다.
③ 제1항 후단에 따라 침해사고의 통지 또는 신고를 받은 관계 기관의 장은 이와 관련된 정보를 과학기술정보통신부장관 또는 한국인터넷진흥원에 지체 없이 공유하여야 한다.
④ 제1항에 따른 신고의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제58조의2(침해사고 신고의 시기, 방법 및 절차) ① 정보통신서비스 제공자는 법 제48조의3제1항 전단에 따라 침해사고를 신고하려는 경우에는 침해사고의 발생을 알게 된 때부터 24시간 이내에 다음 각 호의 사항을 과학기술정보통신부장관 또는 한국인터넷진흥원에 신고해야 한다.
1. 침해사고의 발생 일시, 원인 및 피해내용
2. 침해사고에 대한 조치사항 등 대응 현황
3. 침해사고 대응업무를 담당하는 부서 및 연락처

② 정보통신서비스 제공자는 제1항에 따라 신고한 후 침해사고에 관하여 추가로 확인되는 사실이 있는 경우에는 확인한 때부터 24시간 이내에 신고해야 한다.
③ 제1항 및 제2항에 따른 신고는 서면, 전자우편, 전화, 인터넷 홈페이지 입력 등의 방법으로 할 수 있다.

고로 판단하고 4월 23일 민관합동조사단을 구성[2]하여 피해현황, 사고원인 등을 조사한바, 7월 4일 침해사고 최종 조사결과를 발표하였음[3].

- 민관합동조사단의 조사결과에 따르면 유출된 정보는 전화번호, 가입자 식별번호(IMSI[4]) 등 유심정보 25종이며 유출 규모는 9.82GB, IMSI 기준 약 2,696만건이었음.

- 조사단은 감염서버 중 단말기식별번호(IMEI[5]), 개인정보(이름, 생년월일, 전화번호, 이메일 등)가 평문으로 임시 저장된 서버 2대와 통신기록(CDR[6])이 평문으로 임시 저장된 서버 1대를 발견하였으나, 정밀 분석 결과 방화벽 로그기록이 남아있는 기간(IMEI: 2024. 12. 3.~2025. 4. 24., CDR: 2024. 12. 9.~2025.

---

2) **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4(침해사고의 원인 분석 등)**
① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.
② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자(공공기관등은 제외한다)에게 필요한 조치를 이행하도록 명령할 수 있다.
③ 과학기술정보통신부장관은 제2항에 따른 조치의 이행 여부를 점검하고, 보완이 필요한 사항에 대하여 해당 정보통신서비스 제공자에게 시정을 명할 수 있다.
④ 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생한 경우 제2항에 따른 원인 분석 및 대책 마련을 위하여 필요하면 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.
⑤ 과학기술정보통신부장관은 제2항에 따른 침해사고의 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.
⑥ 과학기술정보통신부장관은 제2항에 따른 침해사고의 원인 분석 및 대책 마련을 하기 위하여 필요하면 정보통신서비스 제공자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 중대한 침해사고의 경우 소속 공무원 또는 제4항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.
3) 과학기술정보통신부 보도자료(2025. 7. 4.) 참조
4) International Mobile Subscriber Identity: 유심 내 저장되며, 통신사가 사용자 식별 시 사용되는 정보
5) International Mobile Equipment Identity: 휴대전화 기기 식별 시 사용되는 정보
6) Call Detail Record: 통화 시간, 수발신자 전화번호 등 통신 활동 관련 정보

4. 20.)에는 자료유출 정황이 없는 것을 확인하였음. 다만, 악성코드 감염시점부터 로그기록이 없는 기간(IMEI: 2022. 6. 15.~2024. 12. 2., CDR: 2023. 1. 31.~2024. 12. 8.)에는 유출여부를 확인하는 것이 불가능하였음.

- 공격자는 시스템 관리망을 통해 저장된 계정 정보를 활용하여 시스템 관리망 내 여러 서버에 악성코드를 설치하고, 서버에 저장된 유심정보를 시스템 관리망 내 외부 인터넷 연결 접점이 있는 서버를 거쳐 유출한 것으로 분석됨.

□ 한편 「개인정보 보호법」에 따르면 개인정보 유출 시 개인정보처리자는 유출된 개인정보 항목, 시점 및 그 경위 등을 정보주체에게 **통지**하고, 유출 피해를 최소화하기 위한 **대책을 마련하고 필요한 조치**를 하여야 함. 또한 개인정보처리자는 개인정보의 유출 사실을 인지한 경우 지체 없이 개인정보보호위원회(이하 "보호위원회"라 함) 또는 한국인터넷진흥원에 유출 관련 사항들을 **신고**하여야 함[7].

---

7) **「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고)** ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

○ 그런데 SKT는 4월 22일 자사 고객의 유심정보가 유출된 정황을 인지하고 보호위원회에 유출신고는 하였으나, 당일 홈페이지에 고객의 일부 정보가 유출된 것으로 추정된다는 내용의 전체 공지만 하였을 뿐, 「개인정보 보호법」에 따른 법정사항을 포함하여 정보주체에게 유출 사실을 개별적으로 통지하지는 않았음[8].

○ 이에 보호위원회는 5월 2일 이번 유출사고로 인한 피해를 최소화하고 개인정보 자기결정권·선택권 보장 및 국민적 불안감을 해소하기 위하여 SKT에 다음과 같은 조치를 즉각 실시할 것을 심의·의결하였고, SKT는 해당 의결사항을 수용하여 5월 9일 유심 관련 개인정보

---

③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

「개인정보 보호법 시행령」 제40조(개인정보 유출 등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.
1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보 또는 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에도 불구하고 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.
③ 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.

8) 당시 SKT는 개인정보 유출 경위 및 항목·규모 등이 확인되지 않아 최초에 개별 유출통지를 진행하지 않았다고 설명한 바 있음.

유출 가능성에 대한 개별적 통지를 문자메시지를 통해 실시하였음.

[보호위원회의 SKT 유출사고 관련 조치요구 의결사항]

○ **첫째, 유출이 확인된 이용자는 물론 유출 가능성이 있는 모든 이용자(SKT 망 사용 알뜰폰 이용자 포함)**에 대하여 법정 사항을 갖추어 신속히 **유출 통지할 것** ○ **둘째,** 고령자·장애인 등 **취약계층**에 대한 **별도의 보호 대책 마련** 및 SKT 전체 이용자의 **2차 피해 예방을 위한 충실한 지원 대책**을 마련할 것 (기존 유심보호서비스, 유심교체 外 이심(esim), 사업자 변경 등 다양한 대책 포함) ○ **셋째,** 이용자의 개인정보 관련 급증하는 **민원에 성실히 대응**하기 위해, **전담 대응팀**을 확대하여 사태가 완전히 해결될 때까지 운영할 것

(자료: "개인정보위, "SKT에 이용자 개인정보 유출 통지 즉각 실시" 의결", 보호위원회 보도자료, 2025. 5. 2.)

○ 보호위원회에서는 5월 20일 개인정보 유출 '가능성'이 아닌 유출 사실에 대한 통지를 실시하도록 개선·보완할 것을 요구하였고, 이에 SKT는 7월 28일 개인정보 유출 사실에 대한 개별 통지를 문자메시지로 실시하였음.

□ 보호위원회는 2025년 8월 현재 「정보통신망법」상 민관합동조사단의 침해사고 조사와 별개로 TF를 구성하여 「개인정보 보호법」에 따른 개인정보 유출조사[9]를 진행중임.

---

9) 보호위원회 조사의 핵심은 (1)개인정보 유출 대상 및 피해 규모의 확정과 (2)사업자의 보호법상 안전조치 의무(기술적·관리적 조치 포함) 위반에 대한 확인임

「개인정보 보호법」 제63조(자료제출 요구 및 검사) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다.
1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 보호위원회는 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관

○ 보호위원회는 자체조사를 통해 SKT의 개인정보 유출 통지 등을 포함한 「개인정보 보호법」 위반 여부를 검토하여 처분할 계획임.

□ 한편 「개인정보 보호법」상 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 정보주체의 수가 50명 이상인 경우 등에는 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 함)에 집단분쟁조정을 신청할 수 있음[10].

○ 분쟁조정위원회의 조정안을 당사자 모두가 수락하면 참여한 모든 신청인에게 효력이 발생하나, 당사자 일방이 불수락하는 경우에

계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.
③ 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위로 인하여 중대한 개인정보 침해사고가 발생한 경우 신속하고 효과적인 대응을 위하여 다음 각 호의 어느 하나에 해당하는 관계 기관의 장에게 협조를 요청할 수 있다.
1. 중앙행정기관
2. 지방자치단체
3. 그 밖에 법령 또는 자치법규에 따라 행정권한을 가지고 있거나 위임 또는 위탁받은 공공기관
④ 제3항에 따라 협조를 요청받은 관계 기관의 장은 특별한 사정이 없으면 이에 따라야 한다.

10) **「개인정보 보호법」 제49조(집단분쟁조정)** ① 국가 및 지방자치단체, 개인정보 보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 "집단분쟁조정"이라 한다)을 의뢰 또는 신청할 수 있다.
② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.
③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.
④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.
⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.
⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.
⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.
⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

는 조정은 불성립함[11].

○ 보호위원회는 6월 19일 SKT 유출사고 관련 집단분쟁조정 2건을 개시하였고, 「개인정보 분쟁조정위원회 운영세칙」에 따라 보호위원회의 조사가 진행되는 기간 동안 조정절차를 일시정지하였다가[12] 조사·처분 완료 즉시 속개하여 조정안을 마련할 계획임.

□ 이렇게 현재 진행되고 있는 절차들에도 불구하고, 개인정보처리자인 SKT의 개인정보 유출 관련 확산 방지노력 등 사후조치가 미흡하다는 지적이 제기되고 있는바[13], 개정안들은 개인정보 유출사고에 따라 권익이 침해된 정보주체의 권리 보호를 담보하기 위하여 개인정보처리자의 개별 통지 의무를 보다 강화하고 후속조치 수립을 의무화하는 등 현행 제도를 보완하려는 것임.

---

11) **「개인정보 보호법」 제47조(분쟁의 조정)** ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.
1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치
② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.
③ 제2항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 수락한 것으로 본다.
④ 당사자가 조정내용을 수락한 경우(제3항에 따라 수락한 것으로 보는 경우를 포함한다) 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인 또는 서명을 한 후 조정서 정본을 지체 없이 각 당사자 또는 그 대리인에게 송달하여야 한다. 다만, 제3항에 따라 수락한 것으로 보는 경우에는 각 당사자의 기명날인 및 서명을 생략할 수 있다.
⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

12) **「개인정보 분쟁조정위원회 운영세칙」 제28조(조정의 일시정지)** ① 위원회는 신청사건과 법률적 및 사실적 쟁점이 동일한 사안에 대한 개인정보 보호위원회의 처분절차가 진행 중인 경우 사실조사를 위하여 필요하다고 인정한 때에는 처분절차가 종료될 때까지 의결을 거쳐 조정을 정지할 수 있다.

13) JTBC뉴스, “SKT, 대처 '미흡' 연속…해킹 경로·피해 규모도 파악 못해”
(https://news.jtbc.co.kr/article/NB12244531)
TV조선, “SKT 해킹으로 2696만건 유출…'보안 미흡' 등 총체적 난국”
(https://news.tvchosun.com/site/data/html_dir/2025/07/04/2025070490271.html)

2. 개인정보처리자의 불법유통 개인정보 모니터링 및 고발 의무화 등(이정문의원안)

□ 개정안은 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우 등으로서 개인정보처리자가 보호위원회 등에 유출 관련 사항을 신고한 경우, 해당 개인정보처리자로 하여금 ① 신고 시부터 2년간 유출등이 된 개인정보가 정보통신망을 통해 불법유통되고 있는지를 모니터링하고 그 결과를 보호위원회에 보고 하도록 의무화하고,

② 불법유통되고 있다고 판단되는 경우 수사기관에 해당 유통자를 고발하도록 의무화하는 등의 내용으로,

국내에 주소 등이 없는 개인정보처리자 중 대통령령으로 정하는 자에 대하여는 해당 규정을 국내대리인에게도 적용하려는 것임(이정문의원안 제31조의2제1항제2호의2 신설, 제34조의3 신설 등).

현 행	이정문의원안
제31조의2(국내대리인의 지정) ① 국내에 주소 또는 영업소가 없는 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 자는 다음 각 호의 사항을 대리하는 자(이하 “국내대리인”이라 한다)를 지정하여야 한다. 이 경우 국내대리인의 지정은 문서로 하여야 한다.	제31조의2(국내대리인의 지정) ① ----------. ----------.

1.·2. (생 략)	1.·2. (현행과 같음)
<신 설>	2의2. 제34조의3제1항 및 제2항에 따른 개인정보 유출 등의 모니터링 및 고발
3. (생 략)	3. (현행과 같음)
② ~ ④ (생 략)	② ~ ④ (현행과 같음)
<신 설>	제34조의3(유출등이 된 개인정보 모니터링과 보고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 제34조제3항에 따른 신고를 한 때에는 신고를 한 때로부터 2년간 유출등이 된 개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7제1항제6호의2에 따른 정보에 해당하는지를 확인하기 위하여 유통 정황 등을 수집·분석하는 개인정보 모니터링을 대통령령으로 정하는 바에 따라 수행하고 그 결과를 보호위원회에 보고하여야 한다. 1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우 2. 민감정보, 고유식별정보가 유출등이 된 경우 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의하여 개인정보가 유출등이 된 경우 ② 제1항에 따라 모니터링을 수행하

	는 개인정보처리자는 유출등이 된 개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7제1항제6호의2에 따른 개인정보에 해당한다고 판단되는 경우에는 수사기관에 그 개인정보를 유통하는 자를 고발하여야 한다. ③ (생 략)
제75조(과태료) ① (생 략)	제75조(과태료) ① (현행과 같음)
② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.	② ----------.
1. ~ 18. (생 략)	1. ~ 18. (현행과 같음)
<신 설>	18의2. 제34조의3제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 유출등이 된 개인정보 모니터링을 수행하지 아니하거나 그 결과를 보고하지 아니한 자
19. ~ 27. (생 략)	19. ~ 27. (현행과 같음)
③ ~ ⑤ (생 략)	③ ~ ⑤ (현행과 같음)

□ 「개인정보 보호법」 제34조에 따르면 개인정보처리자는 개인정보가 분실·도난·유출(이하 “유출등”이라 함)되었음을 알게 되었을 때 지체 없이 해당 정보주체에게 유출 관련 사실을 통지하여야 하고(제1항), 그 피해를 최소화하기 위한 대책을 마련하며 필요한 조치를 취하여야 함(제2항).

또한 개인정보처리자는 유출등을 인지한 때에 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 유출 관련 사실을 지체 없이 보호위원회에 신고하여야 함(제3항)[14].

○ 법 제34조제1항에 따른 유출 관련 통지의무 또는 제3항에 따른 신고의무 위반 시 3천만원 이하의 과태료가 부과되지만, 제2항에 따른 조치의무 위반 시 별도의 제재규정이 부재함[15].

○ 또한 법 제61조는 보호위원회로 하여금 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선

---

14) **「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고)** ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

15) **「개인정보 보호법」 제75조(과태료)** ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.
17. 제34조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
18. 제34조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하지 아니한 자

을 권고할 수 있도록 하고, 권고를 받은 개인정보처리자로 하여금 이를 이행하기 위하여 성실하게 노력할 의무 등을 부과하고 있음[16].

○ 법 제64조는 제61조에 따른 의무 위반을 포함하여 「개인정보 보호법」 위반자에 대하여 보호위원회가 침해행위 중지 등 시정조치를 명할 수 있도록 하고, 시정조치 명령 위반 시 3천만원 이하의 과태료를 부과하고 있음[17].

□ 한편 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 함)」 제44조의7제1항은 정보통신망을 통한 불법정보 유통을 금지하면서, 불법정보의 한 유형으로 '정보통신망법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보'를 규정하고 있음.

---

16) **「개인정보 보호법」 제61조(의견제시 및 개선권고)** ① 보호위원회는 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다.
② 보호위원회는 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 보호위원회에 알려야 한다.
③ 관계 중앙행정기관의 장은 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.
④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

17) **「개인정보 보호법」 제64조(시정조치 등)** ① 보호위원회는 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.
1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치
제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.
27. 제64조제1항에 따른 시정조치 명령에 따르지 아니한 자

○ 이러한 불법정보 유통 시 방송통신위원회는 심의위원회의 심의를 거쳐 해당 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있고, 방송통신위원회의 명령 미이행 시 2년 이하의 징역 또는 2천만원 이하의 벌금에 처해짐[18].

□ 이와 같은 현행 법 체계상 개인정보 유출 시 통지·신고 의무 위반 또는 그 외 「개인정보 보호법」 위반 사실이 있는 경우에는 과태료 부과 및 시정조치 대상이 되고, 개인정보가 정보통신망을 통해 불법유통되는 경우 「정보통신망법」에 따라 포털사이트 운영자, SNS 플랫폼 운영자 등 해당 정보통신서비스 제공자에 대한 해당 정보

---

18) **「정보통신망법」 제44조의7(불법정보의 유통금지 등)** ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.
1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5. 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
6의2. 이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
6의3. 총포·화약류(생명·신체에 위해를 끼칠 수 있는 폭발력을 가진 물건을 포함한다)를 제조할 수 있는 방법이나 설계도 등의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

② 방송통신위원회는 제1항제1호부터 제6호까지, 제6호의2 및 제6호의3의 정보에 대하여는 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다. 다만, 제1항제2호 및 제3호에 따른 정보의 경우에는 해당 정보로 인하여 피해를 받은 자가 구체적으로 밝힌 의사에 반하여 그 처리의 거부·정지 또는 제한을 명할 수 없다.

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
5. 제44조의7제2항 및 제3항에 따른 방송통신위원회의 명령을 이행하지 아니한 자

의 처리 제한 의무 및 제재근거가 마련되어 있기는 하나, 여전히 개인정보 유출사고 발생 시 유출된 정보의 불법거래 등 2차 피해를 방지하기 위한 강제적 조치가 미흡하다는 지적이 제기되고 있음.

○ 특히 2025년 3월 발생한 SKT 개인정보 유출 사태의 경우, 개인정보처리자는 개인정보 유출 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 시행하여야 했으나[19],

SKT가 피해방지 대책으로 마련한 유심보호서비스 및 유심교체는 유심 물량 부족, 서비스 처리지연 등으로 원활하게 이루어지지 않아 국민적 혼란과 불만이 가중된 측면이 있었고, 특히 서비스 가입이나 유심교체가 모바일이나 현장방문을 통해서만 가능하여 고령층·장애인 등 취약계층이 접근하기 어려운 문제가 발생하는 등 유출 피해 방지대책이 미흡하다는 지적이 제기되었음.

□ 이에 개정안은 일정 건수 이상의 개인정보 유출사고가 발생한 경우 등에 개인정보처리자로 하여금 신고일로부터 2년간 불법유통 사이트 등을 모니터링하고 고발 등 후속조치를 수행하도록 함으로써 개인정보처리자의 정보보호 책임을 강화하고 실질적인 피해자 보호를 도모하려는 긍정적인 취지임.

○ 참고로 해외 주요국의 사례는 다음과 같음[20].

---

19) 「개인정보 보호법」 제34조제2항에 근거하여 SKT는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 하나, 이행의 세부기준이 명시되어 있지 않고 이를 위반한 경우에 대한 제재근거는 별도 마련되어 있지 않음.

20) 한국인터넷기업협회 제공자료 재가공

- EU는 GDPR[21]에서 유출사고 발생 시 72시간 이내 감독기관·정보주체 통지, 피해완화조치 이행 등을 명시하고 있으나 구체적인 신용 모니터링[22] 조치가 법적 의무사항으로 규정되어 있지는 않으며 감독기관의 권고 또는 기업의 자율판단에 의해 이루어짐.

- 미국은 캘리포니아를 포함한 일부 주에서 사회보장번호[23] 등 민감정보 유출 시 일정 기간 신용 모니터링 제공을 의무화하고 있고, 대부분의 주에서는 사후조치를 권고하는 수준으로 규정하고 있음.

- 캐나다 개인정보 보호 및 전자 문서법(PIPEDA)에서는 사업자로 하여금 심각한 피해와 실질적인 위험이 있는 침해를 보고하도록 요구하되, 불법유통 사이트 모니터링을 의무화하고 있지는 않음.

□ 다만, 개정안과 관련하여서는 개인정보 유출과 관련된 피해자에 대한 실효적인 보호의 필요성뿐만 아니라 다음 사항을 종합적으로 고려할 필요가 있음.

□ 먼저, 개정안에 따라 불법유통 정황 등에 대하여 모니터링을 실시

21) 유럽 연합(EU)의 개인정보 보호 규정(General Data Protection Regulation)
22) 신용 모니터링(Credit Monitoring): 신용카드 사기, 신분 도용 등 금융 범죄로 인한 피해를 예방하거나 조기에 발견하여 대응할 수 있도록, 개인의 신용 보고서와 관련된 활동을 지속적으로 감시하고, 특이사항이나 의심스러운 활동이 감지될 경우 해당 개인에게 알림을 제공하는 서비스.
23) 사회보장번호(Social Security Number, SSN): 미국에서 개인을 식별하고 사회 보장 혜택 관리 및 세금 관련 업무에 사용되는 번호

하여야 하는 요건이 현행법상 개인정보 유출 신고가 요구되는 경우[24]와 동일한바 사실상 모든 신고 대상 유출사고에 대하여 2년간 모니터링을 실시하여야 하는데, 유출사고의 구체적·개별적 특성을 고려하지 않고 일률적으로 2년간의 모니터링 의무를 부과하는 것이 과도하므로, 이보다는 현행「개인정보 보호법」제64조의 시정조치 규정에 근거하여 사고의 개별적 특성을 감안한 차등적인 규제를 적용하는 것이 더 적절하다는 의견이 존재함.

○ **보호위원회**는 유출신고 대상이라 할지라도 개인정보 유출에 따른 피해 확산 방지를 위하여 필요한 조치는 개별·구체적 사고 내용에 따라 달라지므로[25] 개인정보처리자에게 일률적으로 2년간의 불법유통 개인정보 모니터링 의무를 부여하는 것은 과도한 부담으로 작용할 수 있다는 의견을 제출함.

○ **한국인터넷기업협회**는 현행법상 이미 통지, 신고, 시정명령, 손해배상책임 등의 규정이 존재하고, 기업의 인적·물적 자원은 유한하므로 이러한 일률적인 모니터링은 오히려 데이터 보안 강화 및

24) **「개인정보 보호법 시행령」 제40조(개인정보 유출 등의 신고)** ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.
1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보 또는 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

25) 예컨대 개인정보 유출은 해킹뿐만 아니라 불법유통 가능성이 낮은 1:1 관계의 일시적 주민등록번호 노출 등 양상이 다양할 수 있음.

데이터 침해의 성격을 고려한 구제·예방조치에 활용될 자원을 분산시키고 효율적 자원 배분을 저해할 수 있다는 의견을 제출함.

○ **한국온라인쇼핑협회**는 모든 개인정보 유출사고가 반드시 불법유통으로 이어지는 것은 아니고 2차피해의 실질적 가능성이나 위험은 유출된 개인정보의 항목, 사고의 경위, 사고 후 수습과정 등에 따라 현저히 다를 수 밖에 없으며, 인터넷상 불법거래를 2년간 모니터링하는 것은 기업에 과도한 추가 부담을 초래할 수 있어 과잉금지 원칙에 반한다는 의견을 제출함.

□ 다음으로, 전문기술과 시스템을 보유하지 못한 개인정보처리자가 직접 다크웹 등을 통해 불법유통되는 개인정보를 추적·모니터링하기에는 기술적·현실적으로 한계가 있을 수 있는 점을 고려할 필요가 있다고 보임.

○ 특히 중소기업이 보유한 개인정보가 유출되는 경우, 해당 기업들은 현실적으로 불법유통 개인정보를 모니터링할 자원·역량이 미흡한바 제도의 실효성 확보에 문제가 있을 수 있음.

○ 또한 이미 국가정보원 및 한국인터넷진흥원 등이 다크웹 등에서의 개인정보 불법유통을 모니터링하고 있으므로, 민간기업에 개별적으로 모니터링 의무를 부과하기보다는 기존 기관들의 활동에 대한 지원을 강화하고, 보호위원회 등 공적 기관의 역할을 확대하는 것이 더 효과적이라는 의견[26]도 존재함.

26) 한국온라인쇼핑협회

○ 참고로 보호위원회는 법 제34조의2[27](노출된 개인정보의 삭제·차단)에 따라 온라인상(다크웹 제외)[28] 개인정보 노출 및 불법유통 대응 사업을 수행하고 있으며, 대응 현황은 다음과 같음.

[보호위원회의 개인정보 노출 및 불법유통 탐지·삭제 현황]

(단위: 건)

구분		2020년		2021년		2022년		2023년		2024년	
		탐지	삭제	탐지	삭제	탐지	삭제	탐지	삭제	탐지	삭제
노출	국내	12,033	11,577	14,044	13,619	17,290	16,731	17,848	17,120	17,390	16,569
	국외	3,005	2,939	2,581	2,428	2,076	1,955	3,151	3,044	3,716	3,650
	소계	15,038	14,516	16,625	16,047	19,366	18,686	20,999	20,164	21,106	20,219
불법유통	국내	61,418	57,000	47,003	45,227	48,031	45,360	53,720	51,430	66,782	64,838
	국외	67,111	62,397	93,483	86,769	113,712	107,607	125,418	120,018	111,697	106,526
	소계	128,529	119,397	140,486	131,996	161,743	152,967	179,138	171,448	178,479	171,364
합 계		143,567	133,913	157,111	148,043	181,109	171,653	200,137	191,612	199,585	191,583

주) 대상: 고유식별정보 4종(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호) 및 휴대전화번호, 계좌번호, 신용카드번호, 건강보험번호

(자료: 개인정보보호위원회)

□ 다음으로, 설령 개인정보처리자가 불법유통되는 개인정보를 확인하였다 하더라도 익명성·폐쇄성이 강한 다크웹 등 유통경로의 특성상 해당 정보에 대한 불법유통자, 유통경로 및 구체적인 위반행위를 특정하기 어려운 측면이 있음.

27) **「개인정보 보호법」 제34조의2(노출된 개인정보의 삭제·차단)** ① 개인정보처리자는 고유식별정보, 계좌정보, 신용카드정보 등 개인정보가 정보통신망을 통하여 공중(公衆)에 노출되지 아니하도록 하여야 한다.
② 개인정보처리자는 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우에는 해당 정보를 삭제하거나 차단하는 등 필요한 조치를 하여야 한다.

28) 보호위원회는 다크웹 개인정보 불법유통 대응체계 구축 사업을 신규사업으로 추진 중임.

○ 안 제34조의3제2항은 개인정보처리자가 모니터링 결과 개인정보가 불법유통되었다고 판단되는 경우 수사기관에 해당 유통자를 고발하도록 규정하고 있는데, 개인정보처리자 입장에서는 불법유통되고 있는 개인정보가 확인되더라도 해당 데이터의 출처를 명확히 식별하기 어려운 문제가 있으므로 불법유통자를 실제로 식별하여 고발까지 진행하기에는 현실적인 어려움이 존재할 것으로 예상됨.

□ 마지막으로, 개정안은 모니터링 및 고발 의무 등을 국내대리인에게도 적용하려는 것인데, 해당 사무는 본사에서 처리 가능한 내용으로 국내대리인이 직접 수행하기는 어렵다는 보호위원회의 의견이 제시되었으므로 이를 참고할 필요가 있음.

3. 정보주체의 불법유통 개인정보 신고(이정문의원안)

□ 개정안은 유출등이 된 개인정보로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 정보주체로 하여금 해당 개인정보가 불법유통되거나 된다고 의심되는 경우 보호위원회 등에 신고할 수 있도록 규정하려는 것임(이정문의원안 제34조의3제3항 신설).

현 행	이정문의원안
<신 설>	제34조의3(유출등이 된 개인정보 모니터링과 보고) ①·② (생 략) ③ 유출등이 된 개인정보로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 정보주체는 그 개인정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7제1항제6호의2에 따른 정보에 해당하거나 해당한다고 의심되는 경우 보호위원회 또는 대통령령으로 정하는 전문기관에 신고할 수 있다. 이 경우 신고의 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

□ 현행법 제62조는 개인정보의 처리에 있어서 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해사실을 신고할 수 있도록 규정하고, 보호위원회로 하여금 해당 신고 관련 업무를 효율적으로 수행하기 위하여 전문기관을 지정할 수 있도록 규정함[29].

○ 이에 보호위원회는 개인정보 관련 권익 침해사실의 신고 접수·처리 등을 위하여 한국인터넷진흥원을 전문기관으로 지정하고, 한국인터넷진흥원은 전문기관으로서 "개인정보침해 신고센터"를 운영하고 있음.

[개인정보침해 신고센터 신고·상담 현황]

(단위: 건)

구 분	2019년	2020년	2021년	2022년	2023년	2024년	2025년1분기
신 고	1,041	1,091	7,844	1,923	1,162	762	194
상 담	158,214	176,366	202,923	149,680	108,339	67,613	7,991
합 계	159,255	177,457	210,767	151,603	109,501	68,375	8,185

(자료: 개인정보보호위원회)

29) **「개인정보 보호법」 제62조(침해 사실의 신고 등)** ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다.
② 보호위원회는 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 "신고센터"라 한다)를 설치·운영하여야 한다.
③ 신고센터는 다음 각 호의 업무를 수행한다.
1. 개인정보 처리와 관련한 신고의 접수·상담
2. 사실의 조사·확인 및 관계자의 의견 청취
3. 제1호 및 제2호에 따른 업무에 딸린 업무
④ 보호위원회는 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.

□ 불법유통 피해 확산 방지를 위해 권익을 침해당한 정보주체로 하여금 불법유통 개인정보를 신고할 수 있도록 하려는 개정안의 취지는 타당한 측면이 있으나, 이미 현행법 제62조에서 관련 근거를 마련하고 있으므로 개정 부분의 실익이 크지는 않을 것으로 보임.

4. 개인정보 유출 통지 내용 구체화 및 유출사실 개별 통지 의무화(이해민의원안·최민희의원안)

□ 개정안들은 공통적으로 개인정보가 유출등 된 경우 개인정보처리자가 정보주체에게 알려야 할 사항을 보다 구체화하고,
개인정보가 유출등이 된 정보주체의 범위가 확정되지 않았다 하더라도 유출등의 가능성이 있거나 피해 발생 우려가 있는 모든 정보주체에 대하여 유출등 관련 사실을 개별적으로 통지하도록 하려는 것임(이해민·최민희의원안 제34조제1항제3호, 이해민의원안 제34조제4항 신설, 최민희의원안 제31조의2제1항제2호, 제34조제2항 신설 등).

현 행	이해민의원안	최민희의원안
제31조의2(국내대리인의 지정) ① 국내에 주소 또는 영업소가 없는 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 자는 다음 각 호의 사항을 대리하는 자(이하 “국내대리인”이라 한다)를 지정하여야 한다. 이 경우 국내대리인의 지정은 문		제31조의2(국내대리인의 지정) ① ----------. ----------

서로 하여야 한다. 1. (생 략) 2. 제34조제1항 및 제3항에 따른 개인정보 유출 등의 통지 및 신고 3. (생 략) ② ~ ⑤ (생 략)		----------. 1. (현행과 같음) 2. 제34조제1항·제2항·제4항---------- 3. (현행과 같음) ② ~ ⑤ (현행과 같음)
제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.	제34조(개인정보 유출 등의 통지·신고) ① ----------.	제34조(개인정보 유출 등의 통지·신고) ① ----------.
1.·2. (생 략)	1.·2. (현행과 같음)	1.·2. (현행과 같음)
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보	3. ---------- 관한 구체적인 정보	3. ---------- 관한 구체적인 정보
4.·5. (생 략)	4.·5. (현행과 같음)	4.·5. (현행과 같음)

②·③ (생 략)	②·③ (현행과 같음)	② 개인정보처리자는 유출등이 된 개인정보의 정보주체를 특정할 수 없는 대통령령으로 정하는 규모 이상의 개인정보가 유출등이 된 경우에는 즉시 유출등이 확인된 정보주체 및 유출등의 가능성이 있는 모든 정보주체에게 제1항 각 호의 사항을 개별적으로 알려야 한다. 다만, 같은 항 제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 개별적으로 알려야 한다.
<신 설>	④ 제1항에 따른 유출등의 통지를 다음 각 호의 방법 중 어느 하나 이상의 방법으로 정보주체에게 개별적으로 통지하여야 한다. 이 경우 통지 받을 정보주체의 범위가 확정되지 아니할 경우, 유출된 정보의 성질 및 경로 등을 고려하여 피	

	해가 발생할 우려가 있는 자를 포함한다. 1. 전화 2. 문자메시지 3. 전자우편 4. 서면 5. 그 밖에 정보주체가 쉽게 알 수 있는 방법	
④ (생 략)	⑤·⑥ (생 략)	③~⑤ (생 략)

□ 현행「개인정보 보호법」및 그 시행령에서는 개인정보처리자로 하여금 개인정보 유출등을 인지한 경우 서면등의 방법으로 72시간 이내에 해당 정보주체에게 유출등이 된 개인정보의 항목, 유출등이 된 시점과 그 경위, 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 등에 대한 사항 등(이하 "유출 관련 사실")을 알리도록 규정하면서,

예외적으로 ① 유출 관련 사실에 대한 **구체적인 내용을 확인하지 못한 경우**에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용만이라도 우선 통지하고 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지하도록 하고,

② **정보주체의 연락처를 알 수 없는 경우** 등 정당한 사유가 있는 경우에는 인터넷 홈페이지에 유출 관련 사실을 30일 이상 게시하는 것으로 개별적 통지를 갈음할 수 있도록 하고 있음[30].

○ 그런데 최근 SKT 유심 관련 개인정보 유출사고 발생 직후 SKT는 당사 홈페이지에 고객의 일부 정보가 유출된 것으로 추정된다는 내용의 전체 공지만 하고 유출등이 추정되는 고객들에게 개별적으로 유출 관련 사실을 통지하지 않았으며,

이후 보호위원회로부터 개인정보 유출이 확인되었거나 유출 가능성이 있는 모든 이용자에 대하여 유출 관련 사실을 신속히 개별 통지하라는 권고(5. 2.)가 있자 이를 수용하여 유출 가능성에 대한 개별 통지를 실시하였음(5. 9.).

---

30) **「개인정보 보호법」 제34조(개인정보 유출 등의 통지·신고)** ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

「개인정보 보호법 시행령」 제39조(개인정보 유출 등의 통지) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조 및 제40조에서 "유출등"이라 한다)되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.
1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

② 제1항에도 불구하고 개인정보처리자는 같은 항에 따른 통지를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지해야 한다.

③ 제1항 및 제2항에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다.

- 당시 SKT는 개인정보 유출 경위 및 항목·규모 등이 확인되지 않아 유출사고 직후 개별 유출통지를 진행하지 않았다고 설명한 바 있으나,

  구체적인 유출 범위 등이 확정되지 않은 상황이라 하더라도 정보주체의 개인정보 유출 가능성이 높은 상황에서는 정보주체의 개인정보 자기결정권 보장 및 2차 피해 방지를 위하여 개인정보 유출등 가능성에 대하여 정보주체가 쉽게 알 수 있도록 할 필요가 있다는 의견이 제기되고 있음[31].

○ 이에 이해민의원안은 개인정보가 유출등이 된 범위가 확정되지 않은 경우라 하더라도 유출된 정보의 성질 및 경로 등을 고려하여 피해가 발생할 우려가 있는 경우 해당 정보주체에 대하여도 유출 관련 사실을 전화 등의 방식으로 개별적으로 통지하도록 하려는 것이고,

  최민희의원안은 개인정보가 유출등이 된 범위가 확정되지 않은 경우라 하더라도 대통령령으로 정하는 규모 이상의 개인정보가 유출등이 된 경우에는 즉시 유출등이 확인되었거나 가능성이 있는 모든 정보주체에게 유출 관련 사실을 개별적으로 통지하도록 하려는 것임.

31) SKT의 「개인정보 보호법」 위반 여부에 대하여는 2025년 8월 현재 보호위원회의 조사가 진행 중임.

- 나아가 최민희의원안은 유출 관련 사실에 대한 구체적인 내용을 확인하지 못한 경우 개인정보가 유출등이 된 사실, 그때까지 확인된 내용만이라도 통지하도록 하는 내용을 시행령[32]이 아닌 법률로 상향하여 규정하려는 것임.

○ 또한 두 개정안은 정보주체에게 개별 통지하여야 할 사항으로 '유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보'를 규정하려는 것임.

□ 개정안들은 개인정보의 유출 범위가 명확하지 않더라도 잠재적 피해 가능성이 있는 정보주체를 선제적으로 보호하고 그 알 권리를 보장하기 위한 긍정적인 취지로 보이나, 다음 사항에 대한 검토가 필요할 것으로 보임.

○ 먼저, 이해민·최민희의원안 제34조제1항제3호는 유출등 관련하여 개별 통지하여야 할 사항으로 '유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보'를 규정하고 있는데,

현행법 해석상으로도 유출등 관련 피해를 최소화하기 위해 정보주체가 할 수 있는 방법에 관한 정보의 내용은 정보주체가 이해하고 행동할 수 있을 만큼 구체적이어야 한다는 것이 암묵

32) 현행 법 시행령 제40조제2항에 규정된 내용

적으로 전제되어 있으므로, '구체적인'이라는 문구를 추가하더라도 실제 운영에 있어서 큰 실익이 존재하지는 않을 수 있는 점을 고려할 필요가 있겠음.

○ 다음으로, 두 개정안은 공통적으로 개인정보의 유출등 여부가 명확하게 확인되지 않았더라도 그러한 가능성 또는 피해 우려가 있는 정보주체에 대하여 유출등 관련 사실을 통지하도록 규정하고 있는데, 구체적인 통지 대상에 대한 검토가 필요할 것으로 보임.

- **보호위원회**는 개인정보의 유출등 여부가 명확하지 않더라도 관련 사실을 통지하는 것이 필요하다는 입장으로, 구체적인 통지 대상은 최민희의원안[33]과 같이 '유출 등의 가능성이 있는 모든 정보주체'로 정할 필요가 있다는 의견을 제출하였음.

- **한국인터넷기업협회**는 유출등의 '가능성'이라는 모호한 기준만으로 개별 통지를 시행해야 할 경우 기업 입장에서는 정확하지 않은 정보 제공으로 인해 고객센터 문의 급증, 대내외 혼선, 실제 피해자 대응 역량 저하 등의 부작용이 예상되어 개정안에 대하여 신중한 검토가 필요하다는 의견을 제출하였음.

○ 마지막으로, 최민희의원안 제34조제2항은 '유출등이 된 개인정보의 정보주체를 특정할 수 없는 대통령령으로 정하는 규모 이상의 개인

33) 참고로, 이해민의원안의 경우 '피해가 발생할 우려가 있는 자'를 대상으로 유출 관련 통지를 실시하도록 규정함.

정보가 유출등이 된 경우' 즉시 유출등 관련 사실의 개별 통지를 규정하고 있는데,

유출등이 된 개인정보의 범위를 정확하게 특정할 수 없는 상황에서는 '대통령령으로 정하는 규모'에 대한 판단기준이 명확하지 않을 수 있으므로, 해당 규정의 적용요건이 불분명한 문제가 있을 수 있음.

5. 개인정보 유출 신고기한 단축(이헌승의원안)

□ 개정안은 개인정보처리자가 개인정보의 유출등을 알게 되었을 때 24시간 이내에 유출된 개인정보의 항목 등 법정 사항을 보호위원회 등에 신고하도록 하려는 것임(이헌승의원안 제34조제3항).

현 행	이헌승의원안
제34조(개인정보 유출 등의 통지·신고) ① · ② (생 략) ③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다. ④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.	제34조(개인정보 유출 등의 통지·신고) ① · ② (현행과 같음) ③ ----------제1항에 따른 개인정보의 유출등이----------된 때부터 24시간 이내에----------보호위원회----------. ④ ----------방법----------.

□ 현행법 및 동법 시행령은 개인정보처리자가 개인정보의 유출등을 알게 되었을 때 72시간 이내에 유출등 관련 사실을 보호위원회 등에 신고하도록 규정함[34].

○ 한편 「정보통신망법」 및 동법 시행령에 따르면 정보통신서비스 제공자는 침해사고 발생 시 해당 사실을 알게 된 때부터 24시간 이내에 침해사고 관련 사실을 과학기술정보통신부장관 등에게 신고하도록 규정하고 있는바[35], 유사한 사안에 대한 신고 기한이 상이하게 규정되어 있어 현장에 혼선을 초래할 수 있다는 지적이 존재함.

---

34) **「개인정보 보호법 시행령」 제40조(개인정보 유출 등의 신고)** ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.
1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보 또는 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

35) **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의3(침해사고의 신고 등)** ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.
④ 제1항에 따른 신고의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제58조의2(침해사고 신고의 시기, 방법 및 절차) ① 정보통신서비스 제공자는 법 제48조의3제1항 전단에 따라 침해사고를 신고하려는 경우에는 침해사고의 발생을 알게 된 때부터 24시간 이내에 다음 각 호의 사항을 과학기술정보통신부장관 또는 한국인터넷진흥원에 신고해야 한다.
1. 침해사고의 발생 일시, 원인 및 피해내용
2. 침해사고에 대한 조치사항 등 대응 현황
3. 침해사고 대응업무를 담당하는 부서 및 연락처
② 정보통신서비스 제공자는 제1항에 따라 신고한 후 침해사고에 관하여 추가로 확인되는 사실이 있는 경우에는 확인한 때부터 24시간 이내에 신고해야 한다.
③ 제1항 및 제2항에 따른 신고는 서면, 전자우편, 전화, 인터넷 홈페이지 입력 등의 방법으로 할 수 있다.

○ 이에 개정안은 개인정보처리자로 하여금 개인정보의 유출등을 알게 되었을 때 「정보통신망법」과 동일한 시한인 24시간 이내에 유출 관련 사실을 보호위원회 등에게 신고하도록 규정하도록 함으로써, 보호위원회 등 관계 당국이 보다 조기에 개입하여 정보주체의 보호 및 피해 예방이 신속하게 이루어지는 효과가 있을 것으로 기대됨.

□ 다만, 개정안과 관련하여서는 신중한 검토가 필요하다는 다음 의견을 고려할 필요가 있음.

○ **보호위원회**는 현행 대통령령에서 유출신고 시한을 72시간으로 규정한 것은 침해사고 발생 후 유출 현황, 유출 원인 등을 파악하는 데 소요되는 시간, 피규제자의 과도한 부담 가능성[36], EU 등 글로벌 스탠다드[37] 등을 종합적으로 고려하여 정한 것으로, 「정보통신망법」과 같이 24시간 이내 신고하도록 개정할 경우 수범자 등 법 체계가 상이[38]한 점을 충분히 고려하지 못한 측면이 있고,

통지·신고 시기 등은 사회·기술 수준 등을 고려하여 규정하는 것이 필요한 전문적·기술적 사항으로서 현행과 같이 대통령령에서 규정하는 것이 효율적일 수 있다는 의견을 제출하였음.

36) 정보통신서비스 제공자가 아닌 개인정보처리자의 경우 신고시한을 5일 이내에서 72시간 이내로 단축한 바 있으며(2023년 9월), 아직 제도개선이 이루어진 지 2년이 지나지 않음.
37) EU GDPR은 72시간 이내로, 싱가포르는 3일 이내로 명시함.
38) 개인정보처리자가 정보통신서비스 제공자보다 더 광범위한 개념이며, 「개인정보 보호법」은 해킹 외 모든 유출사고가 대상임.

○ **교육부 및 고용노동부**는 유출신고와 침해사고 신고는 운영 주체·요건 등 법 체계가 상이하고, 기한을 단축할 경우 신고 여부 판단에 과도한 업무부담을 초래할 수 있으므로 신중한 검토가 필요하다는 의견을 제출하였음.

○ **한국인터넷기업협회**는 「정보통신망법」상 침해사고의 신고는 개인정보의 분실·도난·유출 여부와 무관하게 일반적인 침해사고가 발생한 경우 신고하도록 규정한 것이므로 「개인정보 보호법」상 유출사고 신고와는 제도의 취지가 상이하고,

기업 시스템의 고도화로 인한 분산 구조, 클라우드 위탁 처리 등으로 인해 침해사고 발생 시 정확한 분석과 내부 대응에 시간이 소요되는데, 유출사고 발생 인지 후 24시간 이내 정확한 원인 파악, 피해범위 분석, 내부 보고절차 등을 모두 마치고 관계기관에 신고하는 것은 현실적으로 매우 어렵다는 의견을 제출하였음

6. 개인정보 유출 시 후속조치 수립·통지 의무화(이해민의원안)

□ 개정안은 개인정보처리자로 하여금 유출등이 된 개인정보의 삭제·차단 등 확산 방지 조치, 유사 사고의 재발 방지를 위한 대책 등을 포함한 후속조치 계획을 수립하여 보호위원회에 제출하고, 해당 정보주체에게 그 내용을 통지하도록 하며, 위반 시 3천만원 이하의 과태료를 부과하려는 것임(이해민의원안 제34조제5항 신설 등).

현 행	이해민의원안
제34조(개인정보 유출 등의 통지·신고) ①~③ (생 략) <신 설>	제34조(개인정보 유출 등의 통지·신고) ①~④ (생 략) ⑤ 개인정보처리자는 다음 각 호의 사항을 포함한 후속조치 계획을 수립하여 대통령령으로 정한 기한 내에 보호위원회에 제출하여야 하고, 해당 정보주체에게 그 내용을 통지하여야 한다. 1. 유출등이 된 개인정보의 삭제·차단 등 확산 방지 조치 2. 유사 사고의 재발 방지를 위한 대책 3. 정보주체에 대한 피해구제 방안 4. 유출등이 된 개인정보로 인한 추가 피해 발생 여부와 이에 대한 모니터링 계획 5. 그 밖에 보호위원회가 필요하다고 인정하는 사항

④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.	⑥ 제1항 및 제5항에 따른 유출등 및 계획----------.
제75조(과태료) ① (생 략)	제75조(과태료) ① (현행과 같음)
② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.	② ----------.
1. ~ 16. (생 략)	1. ~ 16. (현행과 같음)
17. 제34조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자	17. ---------- 포함한다) 및 제34조제5항----------
18. ~ 27. (생 략)	18. ~ 27. (현행과 같음)
③ ~ ⑤ (생 략)	③ ~ ⑤ (현행과 같음)

□ 개인정보 관련 2차 피해 확산 방지를 위하여 후속조치 계획의 수립 등을 의무화하는 것은 긍정적인 취지로 보임.

○ 다만, 어떠한 경우에 후속조치 계획을 수립하여야 하는지 조문상 불분명한 측면이 있어 이를 보완할 필요가 있음.

○ 또한 보호위원회는 '유사 사고의 재발 방지'의 경우 정보주체의 피해 확산 방지와는 직접적인 관련이 적어 통지 대상에서 제외할 필요가 있다는 의견을 제출하였음.

문 의 처
02)6788-5108