



제433회국회(임시회)
제1차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈 개인정보 국외 이전 시 위원회 심의 의무화 등 〉
■ 최형두의원 대표발의(의안번호 제2216222호)

2026. 3.

정 무 위 원 회
수석전문위원 정 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3
1. 개인정보 국외 이전 시 위원회 심의 의무화 등	3
2. 안전조치 의무의 구체적인 내용을 법률에 명시	8

I. 제안경위

1. 제 안 자: 최형두의원 등 14인
2. 제 안 일: 2026. 1. 22.
3. 회 부 일: 2026. 1. 23.

II. 제안이유 및 주요내용

현행법은 정보주체의 동의를 받거나 개인정보를 이전받는 자가 일정한 보호 조치를 취할 경우 등 제한된 조건에서 개인정보를 국외로 이전할 수 있도록 하고 있음.

그런데 국외로부터의 원격 접속을 통한 개인정보 접근에 대해서는 명확한 규정을 두지 않고 있고, 조건을 충족할 경우 별다른 제한 없이 개인정보의 국외 이전이 가능하여 개인정보의 국외 이전에 대한 보호가 취약하다는 지적이 있음.

또한, 안전성 확보 조치로서 개인정보취급자의 개인정보 접근 권한에 관한 관리가 부실하여 개인정보 유출등의 사건이 빈번하게 발생하는 등 하위법령에 규정된 안전성 확보 조치에 관한 사항 등을 법률로 상향하여 보다 엄격하게 규제할 필요가 있다는 의견이 있음.

이에 위와 같은 제도적 문제점을 개선함으로써 개인정보처리자의 개인정보 보호 의무를 강화하려는 것임.

주요내용은 다음과 같음. 우선, 개인정보를 국외로 이전하는 경우 개인정보 보호위원회의 심의·의결을 거치도록 함(안 제7조의9제1항제6호의2). 둘째, 국외로부터의 원격 접속을 통하여 개인정보에 접근 가능한 경우를 국외 이전으로 보도록 함(안 제28조의8제1항). 셋째, 안전성 확보에 필요한 조치를 법률로 상향하여 명확히 규정함(안 제29조 각 호 신설).

Ⅲ. 검토의견

1. 개인정보 국외 이전 시 위원회 심의 의무화 등

- 개정안은 개인정보를 국외로 이전할 경우 개인정보 보호위원회의 심의·의결을 거치도록 의무화하고, ‘국외로부터의 원격 접속을 통하여 개인정보에 접근 가능한 경우’도 ‘국외 이전’의 범위에 포함하는 내용임 (안 제7조의9제1항제6호의2 및 제28조의8).

현행	개정안
제7조의9(보호위원회의 심의·의결 사항 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. ~ 6. (생략) 6의2. 제28조의9에 따른 개인정보의 국외 이전 <u>중지</u> 명령에 관한 사항 7. ~ 16. (생략) ② ~ ⑤ (생략)	제7조의9(보호위원회의 심의·의결 사항 등) ① ----- -----. 1. ~ 6. (현행과 같음) 6의2. 제28조의8 및 제28조의9----- ----- <u>및 국외 이전 중지</u> -----
제28조의8(개인정보의 국외 이전) ① 개인정보처리자는 개인정보를 국외로 제공(조회되는 <u>경우</u> 를 포함한다)·처리위탁·보관(이하 이 절에서 “이전”이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 <u>개인정보</u> 를 국외로 이전할 수 있다.	제28조의8(개인정보의 국외 이전) ① ----- ----- <u>경우 및 국외로부터의 원격 접속을 통하여 개인정보에 접근 가능한 경우</u> 를----- ----- -----.

현행	개정안
1. ~ 5. (생략) ② ~ ⑥ (생략)	----- <u>보호위원회의 심의·의결을 거친 후에 개인정보</u> ----- ----- 1. ~ 5. (현행과 같음) ② ~ ⑥ (현행과 같음)

□ 국가간 정보 이동이 활발해지고 그 활용도와 중요성이 갈수록 커지고 있는데, 이와 함께 개인정보의 국외 이전 과정에서 개인정보 보호를 강화할 필요성 또한 지속적으로 제기되고 있음.

이에 개정안은 개인정보의 국외이전 시 개인정보보호위원회의 심의·의결을 거친 후에 이전할 수 있도록 하고, ‘국외로부터의 원격접속을 통한 개인정보 접근’을 국외 이전의 범위에 포함함으로써 국외 이전에 따른 개인정보 침해 예방을 더욱 강화하려는 취지로서, 개정안의 내용별 검토의견은 다음과 같음.

□ 첫째, 개정안은 개인정보의 국외 이전 시 보호위원회의 심의·의결을 의무화하고 있음. 현행법상¹⁾ 개인정보의 국외 이전은 ① 정보주체로부

1) 「개인정보 보호법」

제28조의8(개인정보의 국외 이전) ① 개인정보처리자는 개인정보를 국외로 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 절에서 “이전”이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다.

1. 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우
2. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우
3. 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁·보관이 필요한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 제2항 각 호의 사항을 제30조에 따른 개인정보 처리방침에 공개한 경우

터 별도의 동의를 받은 경우, ② 법률 또는 조약에 특별한 규정이 있는 경우, ③ 계약의 체결·이행을 위해 필요한 경우로서 개인정보 처리 방침에 공개하거나 정보주체에게 공개 정보 항목 등을 알린 경우, ④ 개인정보 보호 인증 등을 받은 경우, ⑤ 우리나라와 개인정보 보호 체계 등 보호수준의 동등성이 인정되는 경우에 허용됨.

개정안은 이와 같은 요건을 충족하는 경우에도 개인정보보호위원회의 심의·의결을 거쳐 개인정보의 국외 이전을 허용하도록 하는 내용으로, 개인정보의 국외 이전을 보다 신중하게 결정하도록 함으로써 국외 이전 과정의 개인정보 침해 소지를 최소화하려는 취지로 이해됨.

다만, 개정안에 따르면 정보주체가 스스로 동의하여 개인정보를 국외로 이전하려는 경우에도 보호위원회의 심의·의결을 거쳐야 하는데, 이는 정보주체의 개인정보 자기결정권을 오히려 제약하게 될 소지가 있고, 일상적인 해외 서비스 계약의 체결·이행을 위해 이루어지는 여러 개인정보의 국외 이전에 대해 보호위원회의 심의를 거치도록 하는 것은 사실상 어렵다는 점도 고려할 필요가 있음. 그리고 개정안에 따르면, 다른 법률에서 국외 이전을 허용하는 특별한 규정을 두고 있는 경

나. 전자우편 등 대통령령으로 정하는 방법에 따라 제2항 각 호의 사항을 정보주체에게 알린 경우

4. 개인정보를 이전받는 자가 제32조의2에 따른 개인정보 보호 인증 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서 다음 각 목의 조치를 모두 한 경우

가. 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치

나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치

5. 개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우

우에도 보호위원회의 의결을 거쳐야 할 것으로 보이는데, 「개인정보 보호법」은 개인정보 보호에 관한 일반법²⁾으로서 다른 법률에 특별한 규정이 있는 경우에는 해당 규정이 적용될 것이라는 점을 감안할 때 체계상 적절하지 않은 측면이 있음.

또한, 현행법상 국외 이전을 허용할 수 있는 조건이 되는 개인정보 보호수준의 동등성 인정 등에 대해서는 이미 보호위원회의 심의·의결을 거치고 있어³⁾, 이에 대해서는 중복하여 규정할 실익이 크지는 않아 보임.

□ 둘째, 개정안은 국외 이전의 범위에 ‘국외로부터의 원격 접속을 통하여 개인정보에 접근 가능한 경우’를 포함시키고 있음.

국외 이전은 국내법이 직접 적용되지 않는 국외로 개인정보가 이전되는 것을 의미하고, 국내 또는 국외 중 어디에서 접속하여 개인정보에 접근하는지가 국외 이전의 핵심적인 판단 기준이 되지는 않음. 예를

2) 「개인정보 보호법」

제6조(다른 법률과의 관계) ① 개인정보의 처리 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

② 개인정보의 처리 및 보호에 관한 다른 법률을 제정하거나 개정하는 경우에는 이 법의 목적과 원칙에 맞도록 하여야 한다.

3) 「개인정보 보호법」

제28조의8(개인정보의 국외 이전) ① 개인정보처리자는 개인정보를 국외로 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 절에서 “이전”이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다.

5. 개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우

「개인정보 국외 이전 운영 등에 관한 규정」 [개인정보보호위원회고시, 2023. 10. 16., 제정]

제20조(이전대상국등 인정에 대한 보호위원회 심의·의결) 보호위원회는 제18조에 따른 국외이전전문위원회 평가 내용 및 제19조에 따른 정책협의회 협의 내용 등을 종합적으로 고려하여, 보호위원회의 심의·의결을 거쳐 법 제28조의8제1항제5호에 따라 이전대상국등의 인정 여부를 정한다.

들어 우리나라 국민이 해외 체류 중에 우리나라 개인정보처리자의 온라인 서비스를 원격 접속을 통해 이용한다고 하여 이를 국외 이전의 범위에 포함시키지는 않음. 반면, 우리나라 국민의 개인정보를 외국의 개인정보처리자가 국외에서 원격접속하여 제공받는 경우라면 이는 국외 이전에 해당할 것임.

즉, 개인정보에 대한 접근 방법이 원격인지 여부보다는 국내 법체계가 직접적으로 적용되는지, 국내법에 따른 개인정보 보호 체계가 실질적으로 적용될 수 있는지가 국외 이전의 개념 정의 및 국외 이전에 관한 규율에서 중요한 요소라고 볼 수 있음. 이를 확장하여 원격접속 방법을 통해 정보에 접근하는 일체의 행위를 국외 이전으로 볼 경우 국외 이전에 관한 종래의 개념과 부합하지 않을 수 있다는 점을 고려하여 논의할 필요가 있어 보임.

□ 다만, 현행법상 개인정보의 국외 이전에 관해서는 구체적인 개념이 법률에 구체적으로 제시되어 있지 않다는 개정안의 발의 취지는 타당한 측면이 있으므로, 향후 국외 이전의 개념 등을 법률에서 보다 분명하게 정의하는 방안을 강구할 필요성은 있어 보임.

□ 개정안에 대하여 개인정보보호위원회는 현행법상 요건을 충족한 경우에 대해서 보호위원회의 심의·의결을 거치도록 하는 것은 자기결정권 제한 소지, 타 법률과의 관계 등을 고려할 때 신중한 검토가 필요하고,

원격접속을 통한 접근을 국외 이전에 포함할 실익은 크지 않다는 입장임. 관련 업계⁴⁾의 경우, 현재의 인터넷 환경에서는 대부분의 국가에서 자유롭게 클라우드 등에 접속이 가능하기 때문에 개정안의 취지가 원격접속이라는 접근 방법만을 기준으로 국외이전 여부를 판단하려는 취지라면, 이는 현실과 맞지 않게 그 범위를 지나치게 확장하는 것이고, 이 경우 해외에서의 통상적인 업무에 대해서도 부담이 발생할 것이라는 우려를 제기함.

2. 안전조치 의무의 구체적인 내용을 법률에 명시(안 제29조)

□ 개정안은 개인정보처리자가 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 않도록 하기 위하여 취해야 하는 안전조치로,

데이터베이스시스템에 대한 접근 권한의 부여·변경·말소 등에 관한 기준 수립, 접근 권한이 변경·말소된 개인정보취급자의 개인정보에 대한 접근 권한 제한 조치, 접속기록 보관 및 위조·변조 방지 조치, 개인정보 보호 조직의 구성·운영 등 내부 관리계획 수립에 관한 조치 등을 법률에 명시하려는 내용임(안 제29조 각 호 신설).

4) 한국인터넷기업협회, 한국온라인쇼핑협회

현행	개정안
제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.	제29조(안전조치의무) ----- ----- -----다 음 각 호에 해당하는----- ----- -----.
<신설>	1. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템에 대한 접근 권한의 부여·변경·말소 등에 관한 기준 수립
<신설>	2. 제1호에 따라 접근 권한이 변경·말소된 개인정보취급자의 개인정보에 대한 접근 권한 제한 조치
<신설>	3. 접속기록 보관 및 위조·변조 방지 조치
<신설>	4. 개인정보 보호 조직의 구성·운영 등 내부 관리계획 수립에 관한 조치
<신설>	5. 그 밖에 안전성 확보조치로서 대통령령으로 정하는 사항

- 현행법 제29조에 따르면, 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기

술적·관리적 및 물리적 조치를 하여야 하고,

시행령 제30조에서 내부관리계획의 수립, 개인정보처리시스템에 대한 접근권한의 부여·변경·말소, 접속기록의 보관 및 위조·변조 방지 조치 등에 관한 사항 등을 구체적으로 정하고 있음.

「개인정보 보호법 시행령」

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023. 9. 12.>

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검

가. 법 제28조제1항에 따른 개인정보취급자(이하 “개인정보취급자”라 한다)에 대한 관리·감독 및 교육에 관한 사항

나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항

다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항

2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치

가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 “개인정보처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행

나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영

다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치

3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치

가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치

나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.

다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치

4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치

가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치

나. 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치

다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치

라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치

5. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 다음 각 목의 조치

가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독

나. 개인정보처리시스템에 대한 접속기록의 안전한 보관

다. 그 밖에 접속기록 보관 및 위조·변조 방지를 위하여 필요한 조치

6. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치

7. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

8. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

□ 개정안은 현재 시행령에서 정하고 있는 안전조치 의무의 일부 내용을 법률에 상향하여 규정하려는 내용으로, 개인정보 처리의 안전에 관한 중요한 사항을 법률에서 직접 정하는 것은 수범자의 예측가능성과 명확성 제고 측면에서 긍정적이라 할 것임. 현행법상 안전성 확보에 필

요한 조치를 하지 않은 경우에는 과태료⁵⁾가 부과되고, 안전성 확보 조치를 한 경우에는 과징금 면제 사유에 해당⁶⁾하는 등 제재 규정과도 연계되어 있으므로, 안전조치의 내용을 법률에 명시하는 것은 의미가 있음.

다만, 개인정보 침해 수단과 유형이 갈수록 다양해지고, 보안 환경과 기술의 변화 또한 빠르게 이루어지고 있으므로, 개인정보 보호를 위한 안전성 확보 조치의 구체적이고 세부적인 내용은 하위 법령으로 위임하여 규정할 필요성이 인정될 수 있다는 점도 함께 고려하여 논의할 필요가 있음. 현행법과 유사하게 안전조치의 구체적인 내용을 하위 법령에 위임하고 있는 입법례⁷⁾도 있음.

5) 「개인정보 보호법」

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

6) 「개인정보 보호법」 (2026.3.10. 법률 제21445호로 개정되기 전의 법률)

제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

7) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제23조의6(연계정보의 안전조치 의무 등) ① 본인확인기관이 연계정보를 생성·처리하는 경우 「개인정보 보호법」 제29조에 따른 조치 외에 연계정보 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치를 하여야 한다.

② 연계정보 이용기관은 제23조의5제1항 각 호에 따른 서비스를 제공하는 경우 「개인정보 보호법」 제29조에 따른 조치 외에 연계정보를 주민등록번호와 분리하여 보관·관리하고 연계정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 조치(이하 “안전조치”라 한다)하여야 한다.

③ 방송미디어통신위원회는 생성·처리하는 연계정보의 규모, 매출액 등이 대통령령으로 정하는 기준에 해당하는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치에 대한 운영·관리 실태를 점검할 수 있다. <개정 2025. 10. 1.>

④ 방송미디어통신위원회는 제3항에 따른 점검에 관한 업무를 대통령령으로 정하는 전문기관에 위탁할 수 있다. <개정 2025. 10. 1.>

⑤ 제1항에 따른 물리적·기술적·관리적 조치와 제2항에 따른 안전조치에 관하여 필요한 사항은 대통령

한편, 개정안 제29조 각 호의 내용을 보면, 데이터베이스시스템에 대한 접근 권한에 관한 사항이 특히 강조되어 있는데, 개정안의 취지를 반영할 경우에는 안전 조치의 내용을 주요 유형별로 구분하거나 중요성 등을 고려하여 균형 있게 규정하는 방안도 검토할 필요가 있음.

□ 이와 관련하여 보호위원회는 개정 취지에는 공감하나, 개정 실익은 크지 않다는 입장이고, 한국인터넷기업협회는 세부적이고 기술적인 기준을 법률에 직접 규정할 경우 급변하는 보안 환경에 신속하게 대응하기 어렵다는 의견임.

문 의 처
02)6788-5104

령으로 정한다.

[본조신설 2024. 1. 23.]

「전자금융거래법」

제21조(안전성의 확보의무) ①금융회사등은 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다. <개정 2013. 5. 22., 2020. 5. 19.>

②금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다. <개정 2008. 2. 29., 2013. 5. 22., 2014. 10. 15.>

③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안 기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다. <개정 2014. 10. 15.>

④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.

「의료법」

제38조의2(수술실 내 폐쇄회로 텔레비전의 설치·운영) ④ 제1항에 따라 폐쇄회로 텔레비전이 설치된 의료기관의 장은 제2항에 따라 촬영한 영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 보건복지부령으로 정하는 바에 따라 내부 관리계획의 수립, 저장장치와 네트워크의 분리, 접속기록 보관 및 관련 시설의 출입자 관리 방안 마련 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

【참고자료】 현행법 및 시행령의 안전조치의무 내용과 개정안 비교

현행법	개정안	시행령
내부 관리계획 수립	개인정보 보호 조직의 구성·운영 등 내부 관 리계획 수립에 관한 조 치	○ 내부 관리계획의 수립·시행 및 점검 * 관리·감독 및 교육, 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항 등
접속기록 보관 등	접속기록 보관 및 위조 · 변조 방지 조치	○ 접속기록 보관 및 위조·변조 방지 조치 * 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 ○ 접속기록의 안전한 보관
* 대통령령 으로 위임	데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구 성한 시스템에 대한 접 근 권한의 부여·변경 · 말소 등에 관한 기준 수립 접근 권한이 변경·말 소된 개인정보취급자의 개인정보에 대한 접근 권한 제한 조치	○ 개인정보에 대한 접근 권한을 제한하고 통제하기 위한 조치 * 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템에 대한 접 근 권한의 부여·변경·말소 등에 관한 기준 의 수립·시행 * 정당한 권한을 가진 자에 의한 접근인지를 확 인하기 위해 필요한 인증수단 적용 기준의 설 정 및 운영
	그 밖에 안전성 확보조 치로서 대통령령으로 정하는 사항	○ 개인정보의 안전한 저장·전송에 필요한 조치 * 비밀번호의 일방향 암호화 저장 등 인증정보 의 암호화 저장 등 ○ 악성프로그램의 침투 여부 점검·치료 프 로그램의 설치·운영과 주기적 갱신·점 검 조치 ○ 개인정보의 안전한 보관을 위한 보관시설 의 마련 또는 잠금장치의 설치 등 물리적 조치 ○ 그 밖에 개인정보의 안전성 확보를 위하 여 필요한 조치