



제429회국회(정기회)
제10차 정무위원회

개인정보 보호법 일부개정법률안

검 토 보 고

〈개인정보 암호화 조치 의무화 대상 확대〉

■ 김우영의원 대표발의(의안번호 제2211311호)

2025. 11.

정 무 위 원 회

수석전문위원 정 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견: 개인정보 암호화 조치 의무화 대상 확대	2

I. 제안경위

1. 제 안 자 : 김우영의원 등 16인
2. 제 안 일 : 2025. 7. 7.
3. 회 부 일 : 2025. 7. 8.

II. 제안이유 및 주요내용

현행법은 개인정보처리자로 하여금 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하도록 규정하고 있으며, 필요한 사항에 대하여 대통령령으로 정하는 바에 따르도록 하고 있음.

그런데 이동통신 서비스에서 필수적 정보인 범용 가입자식별모듈에 연계된 정보의 경우 암호화 조치가 의무화되어 있지 않아 가입자식별모듈 침해사고가 발생한 경우 정보주체를 침해 피해로부터 법적으로 보호할 수 있는 근거가 미비함.

이에 개인정보의 암호화 조치 의무화 대상에 가입자식별모듈정보 등 필수적인 개인정보를 규정하여 정보주체의 개인정보를 보다 안전하게 보호하려는 것임(안 제29조).

Ⅲ. 검토의견: 개인정보 암호화 조치 의무화 대상 확대

- 개정안은 개인정보처리자가 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등을 방지하기 위한 안전조치의무에 고유식별정보·생체인식정보·범용 가입자식별모듈정보 등의 개인정보 암호화를 추가하려는 것임(안 제29조).

현행	개정안
제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, <u>접속기록 보관 등</u> 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.	제29조(안전조치의무) ----- ----- ----- ----- <u>접속기록 보관, 고유식별정보·생체인식정보·범용 가입자식별모듈정보 등의 개인정보 암호화 등</u> ----- -----.

- 현행법은 개인정보처리자에게 고유식별정보 및 주민등록번호의 암호화 조치 의무를 직접 법률에서 규정하고 있음(법 제24조제3항1) 및 제24

1) 「개인정보 보호법」

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제 <2013. 8. 6.>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다. (이하 생략)

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느

조의2제2항).

- 일반적으로는 법 제29조를 통해 개인정보처리자에게 안전조치의무를 부여하면서 세부적인 내용을 대통령령으로 위임하고 있으며, 대통령령에서는 일반적인 안전성 확보 조치와 함께 인증정보, 주민등록번호 등 보호위원회가 정하여 고시하는 정보 등의 암호화 저장 등의 조치를 규정하고 있음.

< 개인정보 보호법 시행령 제30조 >

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

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

하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우
- ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다. <신설 2014. 3. 24., 2015. 7. 24.>

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 정보기에 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.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

- 개인정보 보호위원회의 고시는 안전성 확보 조치에 관한 세부 기준을 정하면서, 주민등록번호, 여권번호, 계좌번호, 생체인식정보 등을 암호화하여 저장하도록 규정하고 있음.

< 「개인정보의 안전성 확보조치 기준」 일부 발췌 >

- 제7조(개인정보의 암호화)** ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.
1. 주민등록번호
 2. 여권번호
 3. 운전면허번호
 4. 외국인등록번호
 5. 신용카드번호
 6. 계좌번호
 7. 생체인식정보
- ③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.
1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
 2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)
 - 가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
 - 나. 암호화 미적용시 위험도 분석에 따른 결과
- ④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
- ⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
- ⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

□ 개정안은 이동통신 서비스에서 필수적 정보인 범용가입자식별모듈²⁾에

- 2) 범용가입자식별모듈(Universal Subscriber Identity Module, USIM): 이동통신 네트워크에서 사용자의 신원을 안전하게 인증하고 다양한 기능을 제공하는 스마트카드 기반 모듈로, 사용자 고유번호(예: IMSI, ICCID), 인증키(KI), 통신사 및 요금정보, 연락처·문자·애플리케이션 등 다양한 정보를 저장
- IMSI: International Mobile Subscriber Identity(가입자 식별번호): 통신사가 사용자를 식별하기 위하여

연계된 정보의 경우 암호화 조치가 의무화되어 있지 않아 가입자식별 모듈 침해사고가 발생한 경우 정보주체를 침해 피해로부터 보호할 수 있는 법적 근거가 미비하다고 보아, 고유식별정보·생체인식정보와 함께 가입자식별모듈정보 등을 개인정보의 암호화 조치 의무화 대상으로 법률에 명시하려는 것임.

□ 개인을 식별·인증하고 연결하는 핵심 수단으로 휴대전화가 이용되고 각종 서비스의 본인 확인이 일상화된 상황에서, 이동통신 이용에 필요한 범용가입자식별모듈 정보가 그대로 유출되는 경우 정보주체의 개인정보 침해 뿐 아니라 신원 도용을 통한 2차 피해도 발생할 수 있다는 점에서 이를 예방하기 위해 범용가입자식별모듈 정보를 암호화하도록 명시하려는 개정안의 취지는 타당한 것으로 보임.

○ 지난 4월 SKT 해킹 공격으로 인해 발생한 개인정보 유출 사건에 대한 보호위원회의 조사 결과, SKT 서비스이용자 약 2,300만명의 휴대전화번호, 가입자식별번호(IMSI), 유심 인증키(Ki, OPc) 등 범용가입자식별모듈 정보의 일부가 유출된 것으로 확인³⁾되었고,

유심(USIM)에 저장하는 정보로, 일반적으로 15자리 숫자로 구성됨.

- KI(인증키): 유심카드와 통신사 네트워크가 공유하는 128비트 비밀 암호키로, 이동통신 가입자 인증의 핵심값임. 가입자 인증 과정에서 SIM 내부의 KI와 통신망에 저장된 KI가 대칭 암호키로 사용됨. 유심과 통신망간 보안 및 무결성의 핵심적인 암호키임.
- 사업자 식별자: OP(Operator Code) 특정 이동통신사업자에게 할당된 운영자키로, 그 사업자가 속한 모든 유심에 공통으로 적용되는 값
OPc((Derived Operator Key) OP와 가입자별 KI를 결합하여 생성하는 키로, 각 유심마다 다른 값을 가짐.

3) 개인정보 보호위원회 보도자료, 개인정보위, 'SK텔레콤 개인정보 유출사고' 제재처분 의결, 2025. 8. 28.

○ 특히, SKT가 가입자 인증과 이동통신 서비스 제공에 필수적으로 사용되는 인증정보인 유심 인증키(Ki) 약 2,600만건을 암호화하지 않고 저장·보관함에 따라 유심 인증키가 원본 그대로 유출되어 유심 복제 가능성에 대한 사회적 불안감이 확산되었다는 점에 비추어 볼 때, 범용가입자식별모듈 정보를 암호화하도록 의무화할 필요성이 인정되는 측면이 있음.

□ 다만, 일반적인 법 체계, 법 개정의 실익과 현실적인 어려움 등도 고려하여 신중한 논의가 필요한 것으로 보임.

○ 기술적·관리적 조치의 하나로써 암호화 의무를 법률에 규율할 수는 있으나, 안전성 확보 조치의 하나인 암호화의 구체적 대상을 모두 법률에서 규율하는 것은 법체계⁴⁾상 바람직하지 않은 측면이 있음.

○ 또한, 고유식별정보는 이미 「개인정보 보호법」 제24조제3항을 통해 암호화 등 안전성 확보에 필요한 조치를 하도록 규정되어 있고, 생체인식정보도 「개인정보 보호법 시행령」 제30조제1항제4호 및 「개인정보의 안전성 확보조치 기준」(보호위원회 고시)제7조제1항 및 제2항에서 암호화하도록 규정하고 있어, 법률에 이를 명시할 실익은 크지 않은 것으로 보임.

○ 그 외에, 다양한 정보를 담고 있는 가입자식별모듈에 저장된 모든

4) 전자금융거래법, 위치정보법 등도 구체적인 안전조치는 하위법령에서 정하고 있음

정보를 암호화하도록 하는 것이 기술적·시스템적으로 가능한 것인지에 대한 충분한 검증이 필요한 것으로 보임⁵⁾.

□ 개정안에 대하여 **보호위원회**는 현행 법령 체계로도 고유식별정보 및 생체인식정보에 대해 암호화하도록 규율하고 있어 이를 법률에 별도로 규정할 실익이 크지 않고, 이미 일부 정보(유심 인증키)에 대해서도 「개인정보의 안전성 확보조치 기준」(보호위원회 고시)제7조제1항에 따른 암호화 대상 인증정보에 해당하는 것으로 판단⁶⁾한 점을 고려하여 신중한 검토가 필요하다는 입장임.

□ 개정안에 대하여 **한국인터넷기업협회**에서는 특정 정보 유형을 법률에 직접 명시하는 방식은 신중한 접근이 필요하다는 의견임. 개인정보 보호 관련 기술은 매우 빠르게 발전하며 향후 유사하거나 대체 가능한 식별 수단이 등장할 수 있는데 이때마다 법률 개정이 필요하게 되는 경직성을 초래할 수 있다는 것임.

○ 또한, 가입자식별모듈 관련 정보는 이동통신 서비스의 필수적인 인증 정보로, 네트워크 접속 및 인증 과정에서 실시간으로 이 정보가 사용되는데, 법률로 암호화를 강제할 경우 모든 처리과정에서 암호화 절차를 거치게 되어 데이터 접속 속도 저하 등 전반적인 통신 서비스 품질 저하로 이어질 수 있으며,

5) 주요 통신사들도 가입자식별모듈 보관 정보 중 IMSI 등이 통신망 전반의 정보처리에 사용되므로 암호화가 현실적으로 어렵다는 의견을 보호위원회에 제출함.

6) 개인정보 보호위원회 보도자료, 개인정보위, 'SK텔레콤 개인정보 유출사고' 제재처분 의결, 2025. 8. 28.

- 특히, 이미 국제표준(3GPP)에 따라 통신 규격 자체에 강력한 보안 및 암호화 체계가 적용되어 있어 추가적인 암호화 의무 부과는 실익 보다는 기술적 부담과 시스템의 복잡성을 가중할 우려가 있어, 사업자 부담 및 산업 효율성 저하로 이루어질 수 있다는 의견임.

문 의 처
02)6788-5104