



제 429국회 (정기회)
제 10차 정무위원회

신용정보의 이용 및 보호에 관한 법률 일부개정법률안

검 토 보 고

〈개인신용정보 유출 시 과징금한도 삭제〉

■ 민형배의원 대표발의(의안번호 제2211465호)

2025. 11.

정 무 위 원 회

수석전문위원 정명호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	3

I. 제안경위

가. 제안자 : 민형배의원 등 10인

나. 제안일 : 2025. 7. 14.

다. 회부일 : 2025. 7. 15.

II. 제안이유 및 주요내용

제안이유 및 주요내용

개인신용정보 유출 시, 과징금 한도를 제한한 단서 조항을 삭제하고자 합니다. 제재 실효성을 높이고 소비자 신용정보 보호를 강화하기 위한 것입니다.

현행법상 금융기관은 신용정보시스템에 대한 제3자의 불법 접근, 정보의 변경·훼손 및 파괴 등의 위험에 대비해, 기술적·물리적·관리적 보안대책을 수립·시행해야 합니다. 만약, 개인신용정보가 분실·도난·누출·변조·훼손되면 금융위원회는 과징금을 부과합니다.

과징금 상한이 ‘전체 매출액의 100분의 3 이하’로 정해져 있음에도 불구하고, 단서 조항으로 개인신용정보 유출 등 부과 최대한도가 50억 원으로 제한되어 있습니다. 매출규모가 큰 신용정보회사에는 실질적 제재수단으로 작용하지 못한다는 지적이 있습니다.

유럽의 경우, 2천만 유로(약 270억 규모)와 연간 총 매출액의 4%

중 더 큰 금액을 과징금으로 부과토록 하고 있습니다. 이는 사전규제보다 사후 처벌을 강화해 기업의 실질적인 보안 개선을 유도하고자 하는 취지입니다.

이에, 과징금 한도를 규정한 단서 조항을 삭제하고자 합니다. 제재수단의 실효성을 높이고, 금융소비자의 신용정보를 보다 두텁게 보호하기 위한 것입니다(안 제42조의2제1항).

Ⅲ. 검토의견

☐ 개정안은 신용정보전산시스템의 기술적·물리적·관리적 보안대책의 수립·시행의 미흡으로 인한 개인신용정보의 분실·도난·누출·변조·훼손이 발생한 경우의 과징금 한도인 50억원을 삭제하여 제재수단의 실효성을 제고하려는 것임(안 제42조의2제1항).

현행	개정안
제42조의2(과징금의 부과 등) ① 금융위원회(제45조의3제1항에 따른 상거래기업 및 법인이 다음 각 호의 어느 하나에 해당하는 행위를 한 경우에는 보호위원회를 말한다)는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제1호에 해당하는 행위가 있는 경우에는 50억원 이하의 과징금을 부과할 수 있다.	제42조의2(과징금의 부과 등) ① ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----<단서 삭제>
1. ~ 3. (생략)	1. ~ 3. (현행과 같음)
② ~ ⑨ (생략)	② ~ ⑨ (현행과 같음)

□ **현행 「신용정보의 이용 및 보호에 관한 법률」** (이하 “신용정보법”
이라 함) 제19조제1항¹⁾은 신용정보회사등²⁾이 신용정보전산시스템

제19조(신용정보전산시스템의 안전보호) ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된

을 운용함에 있어 제3자의 불법적인 접근이나 입력된 정보의 훼손·변경·파괴 등을 방지하기 위하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하도록 규정하고 있음.

- 신용정보회사등이 이를 위반하여 개인신용정보를 분실·도난·누출·변조 또는 훼손당한 경우에는 제42조의2제1항제1호에 따라 50억원 이하의 과징금을 부과하도록 규정³⁾하고 있음.

□ 「신용정보법」 상 과징금 제도의 연혁을 살펴보면, 과거 「신용정보법」에는 별도의 과징금 부과 조항이 없고 개인신용정보 유출이 발생하는 경우 이를 유출한 개인에 대해서만 형사처벌 조항이 있었으나, 정보유출이 발생한 신용정보회사등에 대해서도 관리책임⁴⁾을 묻기 위하여 지난 2014년 처음 도입되었음.

- 도입 당시에는 신용정보회사 등이 관리책임 의무 위반으로 갱

정보의 변경·훼손 및 파괴, 그 밖의 위협에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.

- 2) 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관, 신용정보제공·이용자를 의미. / “신용정보회사등”의 현황은 【참고자료】 참조

- 3) 「신용정보의 이용 및 보호에 관한 법률」

제42조의2(과징금의 부과 등) ① 금융위원회(제45조의3제1항에 따른 상거래기업 및 법인이 다음 각 호의 어느 하나에 해당하는 행위를 한 경우에는 보호위원회를 말한다)는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제1호에 해당하는 행위가 있는 경우에는 50억원 이하의 과징금을 부과할 수 있다.

1. 제19조제1항을 위반하여 개인신용정보를 분실·도난·누출·변조 또는 훼손당한 경우
- 4) 지난 2014년에 발표된 카드 3사에서의 대량 개인정보 유출 사건은 카드사의 이상거래탐지시스템(FDS)의 업그레이드를 담당하던 외주업체 직원에 의한 개인정보 유출로, 대법원은 개인의 단순한 일탈이 아니라 카드사들의 USB 반입 통제 미흡·암호화조치 불이행 등을 이유로 카드사들의 죄를 인정한 바 있음.

인신용정보 유출 등이 발생한 경우에는 50억원 이하의 과징금을, 개인비밀을 업무 목적외 누설금지 조항을 위반하여 누설·이용한 경우에는 관련 매출액의 3% 이하의 과징금을 각각 부과할 수 있도록 하였음.

○ 2020년에는 개인신용정보의 오남용을 효과적으로 억제하기 위하여 관련 매출액이 아닌 전체 매출액의 3% 범위에서 과징금을 부과하도록 하였음.

- 다만, 2014년 「신용정보법」에 과징금 제도가 처음 도입될 당시부터 현행 제42조의2제1항제1호 사유⁵⁾에 대해서는 50억원 이하의 과징금 규모는 유지되어 왔음.

【표1】 법 제42조의2제1항 각 호의 과징금 부과 금액

각 호	부과사유	부과금액
1호	·개인비밀을 분실·도난·누출·변조 또는 훼손당한 경우	50억원 이하
1호의2	·신용정보주체의 동의를 받지 않고 개인신용정보를 제3자에게 제공한 경우 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인신용정보를 제공받은 경우	연간 총 매출액의 3% * 매출액 산정 곤란시 200억원 이하
1호의3	·개인신용정보를 목적에 맞지 않게 이용한 경우	
1호의4	·영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리한 경우	
2호	·개인비밀을 업무 목적 외에 누설하거나 이용한 경우	
3호	·불법 누설된 개인비밀임을 알고 있음에도 그 개인비밀을 타인에게 제공하거나 이용한 경우	

5) 기술적·물리적·관리적 보안대책을 위반하여 개인신용정보를 분실, 도난, 누출, 변조 또는 훼손당한 경우

- 금융위원회에 따르면, 2014년 과징금 제도가 도입된 이후 부과된 사례는 총 6건임.

【표2】 신용정보법 제42조의2제1항에 근거한 과징금 부과 현황

부과일	제재기관	부과근거	부과액	비고
2024. 10. 17	AA	제33조제1항 위반 (제42조의2제1항제1의3호)	53.74억 원	
2024. 10. 31	BB	제32조제1항 위반 (제42조의2제1항제1의2호)	1.97억 원	
2024. 12. 03	CC	제42조제1항 위반 (제42조의2제1항제2호)	2.48억 원	
		제19조제1항 위반 (제42조의2제1항제1호)	26.24억 원	50억 한도
2024. 12. 03	DD	제32조제1항 위반 (제42조의2제1항제1의2호)	9.48억 원	
2024. 12. 03	EE	제32조제1항 위반 (제42조의2제1항제1의2호)	10.34억 원	

자료: 금융위원회

- 이와 같이 「신용정보법」 제42조의2제1항 각 호에서 규정하고 있는 과징금 부과 사유에 해당하면 일반적으로 전체 매출액의 3% 범위에서 과징금을 부과하고 있으나, 제1호의 사유에 대해서만 과징금의 상한을 50억원으로 규정함으로 인해 매출규모가 큰 신용정보회사등에는 실질적인 제재수단으로 작용하지 못한다는 지적이 있음.

- 이에 개정안은 「신용정보법」 제42조제1항 단서의 과징금 한도 50억원을 삭제함으로써 개인신용정보의 유출 등에 대한 사후처벌을 보다 강하게 하고, 기업이 개인신용정보를 처리함에 있어 기술적·물리적·관리적 보안대책을 강화하게 하려는 취지로 이해됨.
- 참고로, 「개인정보보호법」 6)에서는 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우7)에는 해당 개인정보처리자에게 전체 매출액8)의 3% 이내의 범위에서 과징금을 부과할 수 있음.
- 유럽연합(EU)의 「일반 개인정보 보호법(GDPR)」의 경우에도 개인정보처리자가 적절한 보안조치를 하지 않아 개인정보가 처리·소실·파기·손상되었을 경우 연간 전 세계 매출액의 4%와 2,000만 유로 중 큰 금액을 과징금으로 부과하도록 규정하고 있음.

6) 「개인정보보호법」

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.

② 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다.

7) 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 제외

8) 다만, 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정

【표2】 유럽연합(EU)의 「일반 개인정보 보호법(GDPR)」 상 과징금 규정

위반행위	과징금 수준
개인정보 처리의 기본 원칙을 위반한 경우 ¹⁾	전 세계 연간 매출액 4% 또는 2천만 유로(약 270억원) 중 더 큰 금액
정보주체의 권리를 보장하지 않는 경우	
제3국이나 국제기구의 수령인에게로 개인정보를 이전할 때 준수해야 할 규정을 위반한 경우	
회원국 법률에 따른 의무를 위반한 경우	
감독기구가 내린 명령 또는 정보 처리의 임시적 또는 확정적 제한에 불복하는 경우, 또는 개인정보 이동 중지 명령을 준수하지 않거나 정보주체의 열람권을 보장하지 않은 경우	

주1) 제5조(개인정보 처리원칙) ① 개인정보는 개인정보의 적절한 보안을 보장하는 방식으로 처리하여야 한다. 보장 방식은 적절한 기술 및 관리적 조치를 사용하여 개인정보가 무단으로 또는 불법적으로 처리된다거나 우발적으로 소실, 파괴, 손상되었을 경우의 보호조치 등을 포함한다.

② 개인정보처리자는 제1항이 준수되도록 할 책임이 있으며, 이를 입증할 수도 있어야 한다.

(자료 : EU 일반 개인정보보호법 가이드북, 한국인터넷진흥원)

- 이러한 외국의 입법례를 비추어 볼 때, 우리나라 역시 기업의 보안 대책 의무 위반에 따른 개인신용정보의 유출 등에 대해서는 보다 강력한 사후처벌을 함으로써 금융소비자의 신용정보를 보다 두텁게 보호하고, 금융거래의 안전을 도모할 필요성이 있다고 보임.
- 아울러, 「개인정보보호법」에서는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 전체 매출액의 3% 이내의 범위에서 과징금을 부과할 수 있도록 규정하고 있다는 점도 과징금 부과 의 형평성 차원에서 고려될 수 있을 것임.

- 다만, 개정안을 논의하는 과정에서 아래와 같은 점을 함께 감안하여 심사할 필요가 있다고 보임.

□ 첫째, 일반적인 개인정보처리자를 대상으로 규율하는 「개인정보보호법」과 달리, 「신용정보법」 상 규율 대상이 되는 ‘신용정보회사등’은 관리책임 의무 위반으로 개인신용정보가 유출된 경우 과징금 외에 「신용정보법」 및 관련 업권 법률에 따라 영업정지, 기관 및 임원 제재 등의 처분이 가능하다는 점을 감안할 필요가 있음.

- 「개인정보보호법」 상 과징금 부과 대상이 되는 ‘개인정보처리자’는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 의미(제2조제5호)하고 있으며, 개인정보처리자가 개인정보를 분실·도난·유출 등을 한 경우 제재수단은 과징금이 사실상 유일함.

- 반면, ‘신용정보회사등’은 개인신용정보를 분실·도난·유출 등을 한 경우 과징금 부과 외에 영업정지⁹⁾, 기관 및 임원 제재¹⁰⁾¹¹⁾

9) 「신용정보의 이용 및 보호에 관한 법률」

제14조(허가 등의 취소와 업무의 정지) ② 금융위원회는 신용정보회사, 본인신용정보관리회사 및 채권추심회사가 다음 각 호의 어느 하나에 해당하는 경우에는 6개월의 범위에서 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다.

4. 제17조제4항 또는 제19조를 위반하여 신용정보를 분실·도난·유출·변조 또는 훼손당한 경우

10) 「신용정보의 이용 및 보호에 관한 법률」

제45조(감독·검사 등) ⑦ 금융위원회는 신용정보회사등이 이 법(채권추심회사의 경우에는 「채권의 공정한 추심에 관한 법률」을 포함한다. 이하 이 항에서 같다) 또는 이 법에 따른 명령을 위반하여 신용정보 관련 산업의 건전한 경영과 신용정보주체의 권익을 해칠 우려가 있다고 인정하면 다음 각 호의 어느 하나에 해당하는 조치를 하거나, 금융감독원장으로 하여금 제1호부터 제3호까지의 규정에 해당하는 조치를 하게 할 수 있다.

1. 신용정보회사등에 대한 주의 또는 경고
2. 임원에 대한 주의 또는 경고

등이 가능함.

- 참고로, 금융위원회는 지난 2014년 3개 신용카드사의 개인신용정보 유출 당시 해당 신용카드 3사에 대해 3개월의 일부 영업정지 처분을 부과한 바 있음.

□ 둘째, 정부는 지난 2025년 10월, ‘범부처 정보보호 종합대책’을 발표하면서 금융위원회도 「전자금융거래법」 개정을 통해 개인신용정보 유출이 반복해서 발생할 경우 과징금을 전체 매출액의 3%로 상향하는 방안을 추진하겠다고 밝힌 바 있음.

- 금융위원회는 신용정보 보호를 두텁게 하기 위한 개정안의 취지에 공감하나, 개인신용정보 등에 대한 해킹 등 방지대책은 「전자금융거래법」 상 안전성의 확보의무¹²⁾를 기반으로 이루어지고 있으므로, 해킹 등으로 인한 개인신용정보 유출 등의 사후처벌 강화는

3. 직원에 대한 주의 및 정직, 감봉, 견책 등의 문책 요구
4. 임원에 대한 해임권고, 직무정지 또는 직원에 대한 면직 요구
5. 위반행위에 대한 시정명령
6. 신용정보제공의 중지

11) 참고로, 「여신전문금융업법」 제24조 및 제57조, 「여신전문금융업법 시행령」 제7조의2 및 「여신전문금융업 감독규정」 등에 따라 신용카드업자가 신용카드회원 등의 신용 관련 자료 등이 외부에 유출된 경우 영업정지 처분이 가능함.

12) 「전자금융거래법」
제21조(안전성의 확보의무) ① 금융회사등은 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다.
② 금융회사등은 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.
「전자금융감독규정」
제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 “금융위원회가 정하는 기준”이라 함은 다음 각 호의 내용에 관하여 제8조부터 제36조에서 정하는 기준을 말한다.
제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.
(각 호 내용 생략)

「전자금융거래법」 개정을 통해 추진할 필요가 있다는 의견을 제시함.

- 이상의 내용을 종합하면, 사후 처벌 강화를 통해 개인신용정보를 보다 두텁게 보호하려는 개정안의 취지는 타당하다고 보이나, 과징금 외의 「신용정보법」 및 관련 업권법에 따른 영업정지 및 기관·임원 제재 처분 제도, 정부의 정보보호 종합대책 입장 등을 종합적으로 고려하여 「신용정보법」 상 과징금 상한을 삭제할지 여부를 논의할 필요가 있음.

문 의 처
02)6788-5106