개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-003-006호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 ㈜섹타나인

의결연월일 2025. 2. 12.

주 문

1. 피심인에 대하여 다음과 같이 과징금, 과태료를 부과한다.

   가. 과 징 금 : 1,477,000,000원

   나. 과 태 료 : 7,200,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인은 처분등에 대한 통지를 받은 날부터 1개월 이내 당해 처분등을 받은 사실 등을 피심인의 홈페이지(모바일 어플리케이션 포함)에 5일 이상 게시하여야 한다. 이때, 구체적인 공표내용과 방법 등은 개인정보보호위원회와 미리 문서로 협의를 거쳐야 한다.

이 유

Ⅰ. 기초 사실

피심인은 등 멤버십 서비스를 제공하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)
㈜섹타나인				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 해킹으로 인해 이용자의 개인정보가 유출된 사실을 인지하고 개인정보 유출신고(1차 : '22. 10. 12., 2차 : '23. 11. 4.)함에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 멤버십 서비스를 운영하면서 '24. 2. 21. 기준 아래와 같이 개인정보를 수집하여 보관하고 있다.

1) 법률 제19234호, 2023. 3. 14. 일부개정, 2024. 3. 15. 시행

< 개인정보 수집현황 >

구분	항목	기간	건수

나. 개인정보 유출 관련 사실관계

1) 유출 경위

해커가 알 수 없는 방법으로 사전에 획득한 이용자의 아이디와 비밀번호를 이용하여 '크리덴셜 스터핑' 공격 방식을 통해 피심인이 운영중인 앱 API에 무차별 대입 공격을 시도하여, '22. 10. 5. ~ '22. 10. 11. 동안 피심인의 시스템에 불법적으로 접근하였고, 국외 IP 주소(6개)를 통해 109,183회 로그인을 시도하여 7,585명의 계정으로 로그인에 성공(성공률 7%) 후 API 응답값에 포함된 개인정보를 탈취하였으며, 이 중 124명의 잔여 포인트를 무단으로 사용*하였다. 이 과정에서 동일 IP에서 로그인 시도 횟수는 최대 1분당 5,063회, 1초당 84회까지 급증하였다.(이하 '1차 사고')

* '22.10.14. 포인트 무단 사용 전수조사 결과, 124명 중 106명에게 포인트 전액을 반환하였고 18명은 사용내역을 취소처리(총 피해액 : 153만원)

해커는 같은 방식으로 '23. 10. 30. ~ '23. 11. 3. 동안 피심인의 시스템에 불법적으로 접근하였고, 국내·외 IP 주소(8개)를 통해 179,310회 로그인을 시도하여 9,762명의 계정으로 로그인에 성공(성공률 5.4%) 후 API 응답값에 포함된 개인정보를 탈취하였으며, 이 과정에서 동일 IP에서 로그인 시도 횟수는 최대 1분당 11,918회, 1초당 198회까지 급증하였다.(이하 '2차 사고')

2) 유출내용

피심인이 운영중인 서비스 회원 17,347명*의 개인정보가 유출되었고, 유출된 정보에는 '아이디, 이름, 포인트 카드번호, 생년, 성별, 잔여 포인트' 등이 포함되어 있었다.

* 1차 : 7,585명, 2차 : 9,762명

3) 유출 인지 및 대응

사고	일 시		유출 인지 및 대응 내용
1차	'22. 10. 11.	09:01	• 포인트 무단 사용 관련 민원* 최초 접수 * 09:25 담당자 전달 이후, 14:28까지 약 5시간 동안 24건, '22. 10. 13. 13:04까지 총 33건의 무단 사용 관련 민원접수
	'22. 10. 11.	14:50~ 18:41	• 로그 분석을 통해 불법 접근 IP 차단
	'22. 10. 11.	18:41~	• 부정 사용 실태 조사
	'22. 10. 11.	21:54	• 비정상 트래픽 인입
	'22. 10. 11.	22:27	• 불법 접근 IP 차단
	'22. 10. 11.	22:38	• 공격자 UA값에서 동일 패턴 반복 확인 및 개인정보 **유출 인지**
	'22. 10. 12.	14:00	• 로그 분석 결과, 10. 5. ~ 10. 11. 크리덴셜 스터핑 공격 확인
	'22. 10. 12.	16:27	• 개인정보 **유출 신고**
	'22. 10. 12.	18:52	• 개인정보 **유출 통지(문자)**
2차	'23. 10. 30.	20:02	• 비정상 로그인 시도에 대한 알람 확인 후 해외 IP 차단 및 **개인정보 유출 인지**
	'23. 10. 30.	20:46~ 21:22	• 추가 공격자 IP 차단
	'23. 10. 30.	23:00	
	'23. 11. 1.	16:00	• 개인정보 **유출 통지**
	'23. 11. 3.	06:37	• 비정상 로그인 시도에 대한 알람 확인 후 국내 IP 차단 및 **개인정보 유출 인지**
	'23. 11. 3.	11:00~ 14:00	• 특정 UA 확인 및 차단

	’23. 11. 3.	18:51~ 18:55	• 비정상 로그인 시도에 대한 알람 확인 후 국내 IP 차단
	’23. 11. 3.	20:00	• 로그인 시 데이터 암호화 적용
	’23. 11. 4.	14:23	• 개인정보 **유출 통지**
	’23. 11. 4.	16:55	• 개인정보 **유출 신고**
	’24. 7. 3.	16:04	• 개인정보 **유출 통지**

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ’16년 5월부터 클라우드 환경에서 사고가 발생한 시스템을 운영하며 침입방지시스템 등 보안장비를 설치하였으나, 1차 사고 당시 동일 IP 주소에서 로그인 시도 횟수가 1분당 최대 5,063회, 1초당 84회까지 증가하였으며, 비정상적인 로그인 시도가 급증하였음에도 이를 즉각적으로 탐지하고 차단할 수 있도록 보안장비에 설정을 적용하지 않고 운영한 사실이 있다.

피심인은 1차 사고 이후 재발방지를 위해 동일 IP에서 내 서로 다른 ID로 회 로그인 시 알람 설정 기능을 마련하였으나, 탐지 후 크리덴셜 스터핑 공격에 대응할 수 있는 차단(대응) 정책을 충분히 마련하지 않은 사실이 있다.

또한, 피심인은 해커의 ‘크리덴셜 스터핑’ 공격으로 앱 API 응답값에 포함된 이용자의 개인정보가 유출되었으나, 이를 예방하기 위한 보호조치 마련을 소홀히 한 사실이 있다.

나. 개인정보 유출 신고·통지 의무를 소홀히 한 행위

피심인은 ’23. 11. 3. 해커의 크리덴셜 스터핑 공격으로 이용자의 개인정보가 유출된 사실을 인지하였으나, 일부 이용자 대상으로 정당한 사유 없이 72시간 경과한 ’24. 7. 3. 유출 통지한 사실이 있다.

또한, 피심인은 ’23. 10. 30. 19:40 해커의 크리덴셜 스터핑 공격으로 이용자의 개인정보가 유출된 사실을 인지하였으나, 정당한 사유 없이 72시간이 경과한 ’23. 11. 4. 16:55 유출 신고한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘24. 9. 4. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’24. 9. 27. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제29조는 “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.”라고 규정하고 있다.

같은 법 시행령[2](이하 ‘시행령’) 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)’, ‘개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷

2) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)

망의 차단(나목)', '그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)'를 하여야 한다."라고 규정하고 있다. 또한, 같은 조 제3항은 "제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다."라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 개인정보의 안전성 확보조치 기준[3](이하 '고시') 제6조1항은 "정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도를 탐지 및 대응(제2호)'하는 등의 안전조치를 하여야"하고, 제6조제3항은 "개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다."라고 규정하고 있다.

나. 보호법 제34조제1항은 "개인정보처리자는 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 '유출등이 된 개인정보 항목(제1호)', '유출등이 된 시점과 그 경위(제2호)', '정보주체가 할 수 있는 방법 등에 관한 정보(제3호)', '개인정보처리자의 대응조치 및 피해 구제절차(제4호)', '정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처(제5호)'를 정보주체에게 알려야 한다."라고 규정하고 있으며, 같은 조 제3항은 "개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다." 라고 규정하고 있다.

또한, 시행령 제39조제1항은 "개인정보처리자는 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항

3) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

각 호의 사항을 정보주체에게 알려야 한다.”라고 규정하고 있으며, 제40조제1항은 “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.” 라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

[보호법 제29조(안전조치의무) 중 접근통제]

개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고 대응하여야 하며, 이러한 보호조치를 이행하였는지 여부는 보편적으로 알려져 있는 정보보안의 기술 수준, 개인정보처리자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등 사정을 종합적으로 고려하여 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다.(대법원 2018. 1. 25. 선고 2014다203410 판결 참조)

피심인은 ’16. 5월부터 클라우드 환경으로 시스템을 이전하면서 침입방지시스템( ) 등 보안장비를 운영하였으나, 1차 사고(’22.10월) 당시 대규모 로그인 시도 등 ‘크리덴셜 스터핑’ 공격에 대응할 수 있도록 비정상적인 접근을 탐지·차단할 수 있는 정책을 운영하지 않은 사실이 확인된다. 이로 인해 피심인은 1차 사고(’22.10.5.~10.11.) 공격 기간 동안 발생한 대량의 로그인 시도를 탐지·차단하지 못하였으며, ’22. 10. 5. 발생한 공격을 약 7일 후인 22. 10. 12. 포인트 무단 사용 관련 민원 분석과정에서 인지하였다.

피심인은 1차 사고 이후 즉시 비정상적인 대규모 로그인 시도 시 탐지(알람)할 수 있도록 임계치를 설정한 정책을 보완한 사실이 확인된다. 다만, 탐지 후 대응(차단) 정책으로 알림을 통해 공격을 인지한 담당자가 직접 시스템에 접속하여 내용을 확인 후 공격자의 IP 주소 등을 차단하는 방식의 대응을 하였으며, 이러한 대응 방식은 '크리덴셜 스터핑' 공격의 일반적인 특징으로 알려진 자동화된 공격 속도(2차 사고 당시 동일 IP 주소에서 1분당 최대 11,918회, 1초당 198회 로그인 시도)에 적합하지 않고, 변칙적인 공격 시간에도 취약하여, 2차 사고('23.10.30.~11.3.) 공격 기간 동안 발생한 대량의 로그인 시도에 즉각적인 대응이 이루어지지 않아 '23.11.3. 04:58 공격 종료 후 약 100분 뒤인 06:37 사후적으로 공격자 IP를 차단하는 등 피심인의 대응은 개인정보 유출을 방지하기 위한 접근통제 조치를 충분히 하였다고 볼 수 없으며, 이로 인해 1차 사고 보다 많은 규모의 개인정보가 또다시 유출되었다.

크리덴셜 스터핑은 국제웹보안표준기구(OWASP) 등으로부터 꾸준히 위험성 및 방어방법이 보고되는 등 널리 알려진 공격 기법이며, 보안업계에서도 충분히 주의와 경각심을 가질 수 있었으므로[4], 평소 동일 IP에서 로그인 시도가 증가하는 시기 및 횟수 등을 분석하여 시스템 보안 정책의 임계치를 설정하는 등 대응 정책을 사전에 마련하였다면 본건과 같은 피해 발생을 회피할 가능성이 있었다고 판단된다.

특히, 법원은 특정 IP의 반복 로그인 시도가 초당 29건 이하인 경우에도 악의적인 행위로 판단하였고[5], 정상 로그인 분석 등을 통해 그에 맞는 룰 세팅을 설정하여 크리덴셜 스터핑에 대응할 수 있다고 판시한 바 있으므로, 피심인은 1차 사고 당시 해커의 로그인 시도 횟수와 일반적인 서비스 이용자의 로그인 시도 횟수 등을 비교하여 1차 사고와 같이 사람이 할 수 없는 속도의 로그인 시도가 인입되는 경우 차단할 수 있도록 룰 세팅을 강화하여 해커의 불법적인 침입을 방지할

4) 법원은 2016년 당시에도 크리덴셜 스터핑이 주의나 경각심을 갖지 못할 정도로 생소한 해킹 공격이라고 보기 어렵다고 판시한 바 있음(서울고등법원 2020.11.4. 선고, 2019누43964)
5) 서울고등법원 2020.11.4. 선고, 2019누43964

필요가 있었다고 판단된다.

한편, 피심인은 NAT 환경에서 접속하는 기업, 단체, 오프라인 매장 등 동일 IP의 대규모 접근이 발생하는 서비스 특성상 임계치를 설정한 차단 정책은 정상적인 접속을 차단할 우려가 있어 차단 정책을 적용할 수 없었다고 주장하나, 피심인이 제출한 자료에 의하면 이용자가 특히 증가하는 기간 동안 NAT 환경의 다량의 로그인 시도 횟수는 크리덴셜 스터핑 공격 당시 로그인 시도 횟수보다 현저히 적은 것으로 확인되고, 피심인은 2차 사고 이후 로그인 시도 시 정책을 도입한 점을 고려할 때, 정상적인 서비스에 대한 오탐 가능성 및 서비스 편의성 저하 등의 이유로 임계치 설정 등 탐지 후 대응(차단)정책을 전혀 적용할 수 없다는 주장은 합리적으로 보이지 않는다.

또한, 피심인이 운영중인 앱 API는 로그인 성공 시 클라이언트에게 아이디, 이름, 생년, 성별, 잔여 포인트, 포인트 카드번호 등 개인정보를 포함한 응답값을 전송하고 있으며, 이미 1차 사고 당시 API 응답값에 포함된 개인정보가 해커에게 유출되었음에도 불구하고 전송되는 데이터를 암호화 하는 등 불법적인 접근에 의해 API 응답값에 포함된 개인정보가 유출되지 않도록 재발방지 대책 마련을 소홀히 하여 동일한 방식으로 이용자의 개인정보가 또다시 유출되었다.

피심인은 2차 사고 발생 이후에야 API 응답값을 암호화 조치하였고, 조치하여 API 호출을 통한 로그인을 차단하였으며 경우에만 로그인 절차가 진행되도록 개선함에 따라 1차 및 2차 사고에 활용된 공격 방식을 차단할 수 있도록 조치하였다.

위와 같은 사유들로 피심인이 API 응답값에 포함된 개인정보를 보호하기 위한 조치를 소홀히하고, 짧은 시간동안 대규모 로그인 시도를 동반하는 '크리덴셜 스터핑' 공격에 대한 탐지·차단 대응 등 개인정보가 유출되지 않도록 보호조치를 소홀히 하여 동일한 유출 사고가 재발하고 이용자 17,347명(1차 사고: 7,585명, 2차 사고 : 9,762명)의 개인정보가 유출된 행위는 사회통념상 합리적으로 기대

가능한 정도의 보호조치를 다하였다고 볼 수 없으며, 이는 보호법 제29조, 시행령 제30조제1항, 고시 제6조제1항 및 제3항을 위반한 것이다.

나. 개인정보 유출 통지·신고를 지연한 사실

[보호법 제34조(개인정보 유출 등의 통지·신고)]

피심인은 ’23. 11. 3. 해커의 크리덴셜 스터핑 공격으로 이용자의 개인정보가 유출된 사실을 인지하였으나, 정당한 사유 없이 72시간 경과한 ’24. 7. 3. 유출 통지한 행위는 보호법 제34조제1항 및 시행령 제39조제1항을 위반한 것이다.

또한, 피심인은 ’23. 10. 30. 19:40 해커의 크리덴셜 스터핑 공격으로 이용자의 개인정보가 유출된 사실을 인지하였으나, 정당한 사유 없이 72시간이 경과한 ’23. 11. 4. 16:55 유출 신고한 행위는 보호법 제34조제3항 및 시행령 제40조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§30① 3호	• 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응을 소홀히 한 행위(고시§6①)
			• 처리하는 개인정보가 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 등에 조치를 취하지 않은 행위(고시§6③)
유출 통지·신고 의무 위반	보호법 §34①	§39①	• 개인정보 유출 인지 후 정당한 사유 없이 72시간을 경과하여 유출 통지한 행위
	보호법 §34③	§40①	• 개인정보 유출 인지 후 정당한 사유 없이 72시간을 경과하여 유출 신고한 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항 제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준[6]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항, 시행령 제60조의2에 따라 위반행위가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 초과하지 아니하는 범위에서 부과할 수 있다.

나. 기준금액

1) 중대성의 판단

과징금 부과기준 제8조제1항은 '시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.'라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 '위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단'하고, '고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.'라고 규정하고 있으며, '고려사항별 부과수준의 판단기준은 ▲(고의 · 과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의

6) 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행)

유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리 · 이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.'라고 규정하고 있다.

피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 '중대한 위반행위'로 판단한다.

2) 기준금액 산출

과징금 부과기준 제6조제1항은 '기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다'라고 규정하고 있다.

피심인의 경우, 과징금 부과기준 제7조제3항에 따라 위반행위가 발생한 서비스 이외에서 발생한 매출은 위반행위와 관련 없는 매출액으로 하고, 직전 3개 사업년도의 연평균 전체 매출액에서 관련 없는 매출액을 제외한 천원에 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 18를 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천 원)

구 분	2021년	2022년	2023년	평 균
①전체 매출액				
②관련 없는 매출액				
①에서 ②를 제외한 매출액				

※ 피심인이 제출한 회계자료를 토대로 작성

<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

다. 1차 조정

과징금 부과기준 제9조에 따라 피심인이 ▲위반기간이 2년을 초과하므로 기준금액의 100분의 50에 해당하는 천 원을 가중하고, ▲위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 기준금액의 100분의 30에 해당하는 금액인 천 원을 감경한다.

라. 2차 조정

과징금 부과기준 제10조에 따라 피심인이 ▲사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우, ▲조사에 적극 협력한 경우에 해당하여 금액의 100분의 20에 해당하는 천 원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2 제1항제9호, 시행령 제60조의2, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 1,477,000천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
			1,477,000천 원

2. 과태료 부과

피심인의 제29조(안전조치의무) 위반행위는 같은 법 제75조(과태료)제2항제5호에 따라 과태료 부과 대상에 해당하나, 제76조(과태료에 관한 규정 적용의 특례)에 따라 과징금을 부과한 행위와 동일하여 과태료를 부과하지 않고,

피심인의 보호법 제34조(개인정보 유출 등의 통지·신고)제1항 및 제3항 위반 행위에 대해 같은 법 제75조(과태료)제2항제17·18호, 시행령 제63조[별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[7](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

가. 기준금액

시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제34조제1항 및 제3항 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 각각 적용한다.

7) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2023. 9. 15. 시행)

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
노. **법 제34조제1항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 **위반**하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제17호	600	1,200	2,400
도. **법 제34조제3항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 **위반**하여 보호위원회 또는 전문기관에 신고하지 않은 경우	법 제75조 제2항제18호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과기준 제8조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반주도 등을 고려하여 가중사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제34조(개인정보 유출 등의 통지·신고)제1항 및 제3항 위반행위에 대하여 가중사유에 해당하지 않아 기준금액을 유지한다.

2) (과태료의 감경) 과태료 부과기준 제7조는 '당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보보호 노력정도, ▲조사협조 및 자진시정 등을 고려하여 감경사유가 인정되는 경우)에 따라 기준금액의 100분의 90의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제34조(개인정보 유출 등의 통지·신고)제1항 및 제3항 위반행위에 대하여 ▲사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우(20% 이내), ▲조사에 적극적으로 협력한 점(20% 이내) 등을 종합적으로 고려하여 과태료 부과기준 제7조에 따라 기준금액의 40%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제34조제1항 및 제3항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
유출 통지 의무	600만 원	-	240만 원	**360만 원**
유출 신고 의무	600만 원	-	240만 원	**360만 원**
계				**720만 원**

3. 처분 결과 공표명령

피심인의 위반행위는 보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」[8](이하 '공표 및 공표명령 지침') 제6조제1항제5호·제7호·제9호 해당하고 위반행위가 인터넷을 통하여 이루어졌으므로, 제8조 및 제11조에 따라 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 5일 이상 7일 미만의 기간 동안(휴업일 포함) 공표하도록 명한다.

이때 제7조제1항, 제8조제3항에 따라 원칙적으로 공표지침 [별표]의 표준 공표 문안을 따르되, 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 하고, 제11조제3항에 따라 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

8) 개인정보 보호법 위반에 대한 공표 및 공표명령 지침(개인정보보호위원회 지침, 2023. 10. 11. 시행)

이의제기 방법 및 기간

피심인은 이 과징금 부과처분, 공표명령에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2025년 2월 12일

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)