개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-013-043호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

대표자
의결연월일 2025. 6. 11.

주 문

1. 피심인에게 다음과 같이 시정조치를 명한다.

가. 향후 개인정보 유출 사고를 예방할 수 있도록 내부 개인정보 보호 체계를 정비하는 등 재발방지대책을 수립·시행하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대한 시정명령의 내용을 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 가맹점을 대상으로 온라인 결제대행 서비스를 제공하는 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 정보통신서비스 제공자이며, 피심인의 일반 현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('22. 7. 19.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 4. 26. ~ '24. 12. 31.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 가맹점 대상 온라인 결제대행 서비스를 제공하면서 '22. 8. 5. 기준으로 이용자 건의 개인정보를 수집하여 보관하고 있다.

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

< 개인정보 수집현황 >

구분	항목	수집일	건수(명)
합 계			

나. 개인정보 유출 관련 사실관계

신원 미상의 자(이하 '해커')는 '22. 6. 9. 14:10 피심인의 웹 관리자 페이지( ) 접근 후 사전에 획득*한 가맹점 계정정보로 로그인하여, 관리자 페이지 내 개인정보가 포함된 2개 페이지** 접근 및 개인정보를 조회하였다.

*

** 페이지(구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))
페이지(사업자명, 구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))

이후, 해커는 '22. 6. 9. ~ 6. 13. 피심인 웹 관리자 페이지에 SQL 인젝션 공격 및 관리자 계정정보 획득 및 로그인하여, 관리자 페이지 내 개인정보가 포함된 2개 페이지* 접근 및 개인정보 조회함

* 페이지(구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))
페이지(사업자명, 구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))

1) (유출 내용) 해커가 접근한 2개 웹페이지를 기준으로 각 첫페이지에 노출되는 이용자 최소 80명*의 개인정보

* 60명(구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))
20명(사업자명, 구매자명, 구매자 휴대전화번호, 카드번호(가운데 4자리 마스킹))

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용
’22. 6. 28.	가맹점(　　)으로부터 개인정보 유출 확인 요청 연락 수신
’22. 7. 4. ~ 7. 6.	한국인터넷진흥원에 중소기업 침해사고 피해지원 신청
’22. 7. 6.	가맹점에 해킹 공격 사실 안내 공지
’22. 7. 19. 10:31	한국인터넷진흥원으로부터 침해사고 분석보고서 수신 및 유출 인지 ※ 분석결과, 해커는 온플랫 관리자페이지 접근 및 이용자 개인정보 유출
‘22. 7. 19. 15:31	개인정보 포털에 개인정보 유출 신고
‘22. 7. 19.	관리자 페이지 접속 시 사내 IP 이외 모든 IP 차단 조치
‘22. 9. 26.	기존 시스템(서버, DB, 관리자페이지 등)에서 클라우드(　　) 시스템 이관 ※ IP 제한, 2차 인증, 접속기록 보관 등 조치 실시

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ‘19. 12. 10.부터 외부에서 정보통신망을 통해 개인정보처리시스템인 웹 관리자 페이지 접속 시 안전한 인증수단 적용 없이 아이디·비밀번호만으로 접속이 가능하도록 운영하였고, 해당 접속 권한을 IP 주소 등으로 제한하지 않았으며, SQL 인젝션 쿼리와 같은 이용자 입력값에 대한 검증 등 조치를 하지 않은 사실이 있다.

피심인은 ‘19. 12. 10.부터 웹 관리자 페이지에 대한 개인정보취급자가 접속한 기록을 보존·관리하지 않았으며, 관리자 및 개인정보취급자의 계정의 비밀번호를 일방향 암호화하지 않고 평문으로 저장한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’25. 3. 19. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’25. 3. 31. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 舊 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 ‘舊 시행령’) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 이 조에서 ”개인정보처리시스템“이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(가목)’, ‘개인정보처리시스템에 대한 침입차단 시스템 및 침입탐지 시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제48조의2제1항제3호는 “접속기록의 위조·변조 방지를 위해 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제48조의2제1항제4호는 “개인정보가 안전하게 저장·전송될 수 있도록 하기 위해 ‘비밀번호의 일방향 암호화 저장(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

기준') 제4조4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다."라고 규정하고 있고, 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(1호) 및 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있고, 제4조제9항은 "정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

舊 기술적 보호조치 기준 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다."라고 규정하고 있고, 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 외부에서 정보통신망을 통해 개인정보처리시스템인 웹 관리자 페이지 접속 시 안전한 인증수단 적용 없이 아이디·비밀번호만으로 접속이 가능하도록 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제4항을 위반한 것이다.

피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템인 웹 관리자 페이지에 대한 접속 권한을 IP 주소 등으로 제한하지 않아 인가받지 않은 접근을 허용한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제5항을 위반한 것이다.

피심인이 SQL 인젝션 쿼리와 같은 이용자 입력값에 대한 검증 등 접근통제 조치를 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

피심인이 웹 관리자 페이지에 대한 개인정보취급자가 접속한 기록을 보존·관리하지 않은 행위와 관리자 및 개인정보취급자 계정의 비밀번호를 일방향 암호화하지 않고 평문으로 저장한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제5조제1항 및 제6조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호·제3호·제4호	• 정보통신망을 통해 외부에서 개인정보처리시스템 접속 시 안전한 인증수단 미적용(舊 기술적 보호조치 기준 §4④) • 불법적인 접근 및 침해사고 방지를 위한 개인정보 처리시스템에 대한 침입 탐지·차단 시스템 운영 소홀 (舊 기술적 보호조치 기준§4⑤) • 열람 권한이 없는 자에게 유출되지 않도록 필요한 조치를 취하지 않은 행위(舊 기술적 보호조치 기준§4⑨) • 개인정보취급자가 개인정보처리시스템의 접속기록을 보존·관리하지 않은 행위(舊 기술적 보호조치 기준§5①) • 비밀번호를 복호화되지 않도록 일방향 암호화하여 저장하지 않은 행위(舊 기술적 보호조치 기준§6①)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 향후 개인정보 유출 사고를 예방할 수 있도록 내부 개인정보 보호 체계를 정비하는 등 재발방지대책을 수립·시행하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 결과 공표

舊 보호법 제66조제1항 및 舊 개인정보 보호위원회 처분결과 공표기준[4](이하 '舊 공표 기준') 제2조(공표요건)에 따르면 피심인의 위반행위는 '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로 舊 보호법 제66조제1항에 따라 피심인이 과태료 부과를 받은 사실에 대해 개인정보보호위원회 홈페이지에 1년간 공표한다.

※ 질서위반행위규제법에 근거하여 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」에 따라 공표기간 1년을 소급 적용

개인정보 보호법 위반 행정처분 결과 공표

개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		舊 보호법* 제29조	안전조치의무	2025. 6. 11.	시정조치 명령

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2025년 6월 11일

개 인 정 보 보 호 위 원 회

4) 개인정보보호위원회지침, 2020. 11. 18. 시행

이의제기 방법 및 기간

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

이상과 같은 이유로 주문과 같이 의결한다.

2025년 6월 11일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 환 (서 명)

위 원 김 휘 강 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)