개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2023-012-153호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 ㈜엘지유플러스 (사업자등록번호 :)

대표자

의결연월일 2023. 7. 12.

주 문

1. 피심인 ㈜엘지유플러스에 대하여 다음과 같이 시정조치를 명한다.

가. 운영 중인 개인정보처리시스템 전반에 대해「개인정보 보호법」제29조(안전조치 의무), 같은 법 시행령 제48조의2(개인정보의 안전성 확보조치)를 준수하고 취약 부분을 개선할 것

나. 전사적 차원에서 개인정보 내부관리계획(거버넌스)을 재정립(권한·책임 명확화)할 것

다. 개인정보 보호책임자의 역할과 위상(CEO 직속 조직구성 등) 및 전문성을 강화 할 것

라. 전 직원을 대상으로 정기적인 개인정보 보호 교육 계획을 수립하고 실시할 것

마. 개인정보처리시스템 내에 법령상 보관 의무가 없거나 처리 목적 달성 등으로 불필요하게 보관하고 있는 개인정보를 모두 파기할 것

바. 피심인은 가.부터 마.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 90일 이내에 이행결과를 개인정보보호위원회에 제출할 것

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 6,800,452,000원
나. 과 태 료 : 27,000,000원
다. 납부기한 : 고지서에 명시된 납부기한 이내
라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

유·무선통신업 등을 운영하는 피심인은 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다.)에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보종합포털(privacy.go.kr)에 유출 신고('23. 1. 3.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 1. 9. ~ '23. 6. 19.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 유·무선통신업을 운영하는 사업자로, ’23. 6. 30. 기준으로 아래와 같이 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
이용자 DB (Ucube DB)		’90. 1. 1. ~ ’23. 6. 30.	
해지 DB		’90. 1. 3. ~ ’23. 1. 24.	
고객인증 DB (CAS DB)		’97. 12. 12. ~ ’23. 6. 30.	

나. 운영 중인 시스템 현황

신원미상의 자(이하 ‘해커’)가 공개한 정보를 피심인이 보유한 고객정보와 비교한 결과, 유출된 개인정보는 피심인의 서비스 이용자의 개인정보임을 확인*하였고, 해당 정보의 출처는 ‘고객인증시스템(CAS)’의 DB**임을 확인하였다.

* 항목 중 @ez-i.co.kr / lte-lguplus.co.kr 등 도메인 사용, U+인터넷전화 등 상품명 사용, 일부 암호화된 비밀번호 및 암호알고리즘(AES128)으로 암호화된 주민등록번호의 값이 일치

** 해커가 공개한 항목 26개 중 22개 항목이 일치, 나머지 중 3개는 유사

피심인은 수집된 이용자의 정보를 이용자(Ucube) DB, 고객인증시스템(CAS) DB, 해지 이용자 DB에 보관 중이며, 고객인증시스템(CAS)은 피심인의 일부 서비스( )에 대한 부가서비스 가입과 해지를 위해 이용자 정보를 저장·관리하는 것으로 확인되었다.

*

피심인이 운영하는 고객인증시스템(CAS)은 개발기·검수기·운영기로 구분되며, 모두 유사한 환경(Web/WAS/DB, 인증관리/인증처리/인증DB)으로 구성하여 개발, 테스트, 서비스 제공 등을 위해 운영하는 것으로 확인되었다.

고객인증시스템(CAS)을 확인한 결과, 테스트 등을 위해 운영기 DB에서 개인정보를 추출하여 서버(프록시)를 통해 개발기로 전송하거나, 주기적( )으로 다른 서버(대외GW)에 개인정보를 전송한 사실*이 확인되었으며,

* 개발자용 보안 클라우드에서 프록시 서버( )를 통해 CAS 운영기에서 개발기로 전송('22.9.21.), CAS 운영기의 DB 자료는 대외 게이트웨이(GW)로 자동 전송('15.12.~ '21.6. 매달), 대외 GW에서 다른 서버로 DB 파일 전송('18. 2. 10., '19. 1. 17.등)

운영기에서 개발기·검수기로 옮겨진 약 1,030만 건(개발기에 약 115만 건, 검수기에 약 915만 건)의 개인정보가 '23. 1월 조사 시점까지 남아 있었다. 피심인은 서버 접근제어와 DB 접근제어 시스템을 이용하여 최근 5년간 접속기록을 보관하고 있으나, 개발기·검수기에 남겨진 대량의 개인정보를 추출한 기록을 확인할 수 없었다. 피심인은 해당 파일을 누가, 어떤 목적으로 개발기·검수기로 옮겼고 '23. 1월까지 남아 있는 사유 등에 대해 소명하지 못하는 등 구체적인 개인정보 추출·전송에 대한 수행업무와 같은 접속기록을 남기지 않아 대규모 개인정보 추출 등에 대한 이상 유무 점검·확인 등의 관리통제가 되지 않은 사실이 있다.

※ 피심인은 DB서버에 직접 접속하거나 서버 간 연결 방식으로 개인정보 조회, 다운로드 등 실행 시 수행한 행위(조회 건수 등)는 기록되지 않는 방식으로 운영하는 것으로 확인됨

- 운영기 DB의 자료 자동 전송('15.12.~ '21.6. 매달)과 관련한 개인정보 추출 기록을 DB 접근제어에서 확인할 수 없었으며, 피심인은 서버 접근제어 시스템의 기록으로 사용자가 이용한 명령어는 확인할 수 있다고 소명

또, 피심인이 운영하는 고객인증시스템(CAS)은 운영체제(OS), DB관리시스템(DBMS), 응용프로그램용 상용소프트웨어(WEB, WAS) 대부분이 '18. 6월을 기준으로 단종 혹은 기술지원 종료 상태(OS를 제외한 DBMS, WEB, WAS 등은 기술지원 종료)로 조

사 시점인 ‘23. 1월까지 유지되고 있었으며, 일부 소프트웨어는 ’12. 9월부터 기술지원 종료 상태로 ‘23. 1월까지 운영 중인 사실을 확인하였다.

아울러, 불법침입 및 침해사고 방지를 위한 침입차단시스템(방화벽), 침입방지시스템(IPS), 웹방화벽 역시 ’18. 6월 기준으로 일부는 단종 또는 기술지원이 종료된 상태였으며, ‘23. 1월 조사 시점에는 모든 방화벽·IPS·웹방화벽이 단종 또는 기술지원이 종료되거나 정상적인 운용으로 보기 어려운 상태로 확인되었다. 운영기 방화벽은 제조사에서 ’17. 6월 단종하고 ‘22. 6월에 기술지원도 종료한 상태였으며, 개발기·검수기 방화벽은 제조사에서 ’20. 12월 단종, ‘23. 12월에 기술지원도 종료할 예정으로 확인되었다. 운영기 침입방지시스템은 제조사에서 ‘22. 6월 기술지원을 종료한 상태였으며, 개발기 IPS는 ’17년 이후부터 IPS를 교체한 ‘23. 4월까지 공격 탐지 패턴 업데이트가 전혀 없었다. 개발기·검수기도 웹 서비스를 운영 중이나 웹방화벽은 설치하지 않았고, 운영기 웹방화벽은 ’17. 4월 이후 공격 탐지 패턴 업데이트가 없었으며, 피심인은 운영기 웹방화벽을 단종된 제품이라고 소명한 사실이 있다.

피심인이 설치·운영 중인 운영기·개발기의 방화벽은 IP 주소 제한 기능 이외에 침입방지, 안티바이러스 등 여러 기능을 포함한 제품이었으나, 피심인은 안정적인 서비스 운영을 위해 IP 주소 제한 기능만 적용하고 있다고 소명한 바 있다.

피심인이 자체적으로 실시한 ‘18년 점검에서도 고객인증시스템(CAS)의 전체적인 노후화 사실을 지적하고 시스템 교체 및 성능개선을 권고하였으나, ’23. 1월까지 이행하지 않은 사실이 있다.

피심인은 개발기 방화벽을 운영하면서 개발자의 요청(‘15. 6. 3., ’16. 4. 19., ‘22. 7. 27. 등, 특정 IP에서 개발기로 접속 허용 요청)으로 일시적으로 외부 IP 주소에서 개발기 서버

로 접근을 허용하는 정책을 방화벽에 등록하였으나, ’23. 1월 조사 시점까지 해당 정책을 변경하지 않고 유지한 사실을 확인하였다. 특히, 개발자는 특정 IP 주소에서 개발기로 접속 허용을 요청하였으나, 개발기 방화벽 정책에는 어디(Any)에서든 포트로 접속을 허용하는 정책을 등록하였고, 해당 작업이 종료됐음에도 ’23. 1월 조사 시점까지 해당 정책을 변경하지 않고 유지한 사실을 확인하였다.

아울러, 고객인증시스템(CAS) 개발기에 ‘09년과 ’18년에 업로드된 악성코드(웹셸)가 ‘23.1월 조사 시점까지 삭제되지 않고 남아 있었으며,

* ’23.1월 조사 당시에는 웹서비스 경로가 변경되어 ‘09년, ’18년도 웹쉘이 실행 불가능하였으나, ’18. 6. 29. 웹로그를 삭제하여 업로드 시점의 실행 가능 여부는 확인되지 않음

잔존 웹셸에 대한 보안장비 탐지 시연(’23. 4. 13.)에서 개발기 IPS는 해당 웹셸을 정상적으로 탐지하지 못한 사실이 있다.

* 시연에 **활용된 웹셸은 ’04.4월에 공개** 배포한 웹셸로, 국내외 바이러스 백신과 무료/상용 보안제품에서 탐지·차단할 수 있는 웹셸로 확인됨

* ‘18.6월 기준으로 개발기 방화벽은 포트로 외부 접속을 모두(Any) 허용, 개발기 IPS는 8081 포트에 대한 모든 웹셸 탐지정책 미적용 등 포트로 제공하고 있는 **웹서비스에 대한 웹셸 공격에 대한 탐지·차단이 어려운 상태임을 확인함**

* 피심인은 웹셸 점검 도구를 ’16년 도입하였으나, 개발기는 점검 이력이 없고, 검수기는 ‘21년에 점검한 이력이 있었음

다. 개인정보 유출 관련 사실관계

1) 유출 경과 및 대응

일 시	피심인의 유출인지 및 대응 내용
’23. 1. 1.	미상의 해커가 해킹포럼에 피심인의 고객정보 판매글을 게시(샘플 31건)
’23. 1. 2.	KISA의 확인 요청으로 유출 인지, 해커로부터 샘플(599,148건) 입수
’23. 1. 3.	개인정보보호 포털(privacy.go.kr)에 유출 신고(샘플 31건)

일 시	피심인의 유출인지 및 대응 내용
’23. 1. 4.	해킹포럼 관련 정보주체에게 유출 사실 통지(이메일)
’23. 1. 5.	피심인의 2차 개인정보 유출 신고(599,148건)
’23. 1. 9.	피심인의 3차 개인정보 유출 신고(‘23.1.7. 송부받은 812건)
’23. 1. 10.	정보주체에게 유출 사실 통지 187,3784건(이메일·문자·우편, 홈페이지 공지)
’23. 1. 16.	신원미상의 자가 중국 텐센트 클라우드 홈페이지에 동일정보 공개(253건)
’23. 1. 17.	피심인의 4차 개인정보 유출 신고(7건 추가 확인, 중복제거시 4건)
’23. 1. 20.	피심인의 5차 개인정보 유출 신고(CAS DB에서 3만 건 추가 확인)
’23. 1. 31.	피심인의 6차 개인정보 유출 신고(해지 이용자 DB에서 8만건 추가 확인)
’23. 2. 3.	피심인의 5차, 6차 신고건에 대한 유출 통지(11만 건) ※ 해지 이용자 DB(81,586건)와 CAS DB에서 확인(28,043건)된 이용자 대상 유출 통지

2) 유출항목

휴대전화번호, 교환기주소, 고객번호, 성명, 우편번호, 주소, 생년월일, 전화번호, 주민등록번호(암호화), IMSI(국제 모바일 가입자 식별자), 입력시간, 수정시간, 모델명, 이메일, 비밀번호(암호화), 최초가입일자, USIM고유번호, IMEI(국제 휴대전화 식별번호), MAC주소, 아이디, 서비스명 등(일부 칼럼은 내용 중복) 26개 항목이 유출되었다.

3) 유출규모 및 유출시기

이용자의 개인정보 총 297,117건(고객번호 기준)이 ’18.6.15. 이후 유출되었다.

* 해커가 공개한 데이터 600,562건(중복 제거시 297,516건)과 비교한 결과, 총 297,117건의 개인정보가 확인(399건 확인불가)되었으며, 해커가 공개한 정보 중 유출 시점을 추정할 수 있는 ‘UPDATE_DTIME’의 데이터 중 고객인증(CAS) DB와 일치하는 데이터의 가장 최근 일자가 ‘2018/06/15 03:23:33’이었다.

3. 개인정보의 취급.운영 관련 사실관계

가. 불필요하게 된 개인정보를 파기하지 않은 행위

피심인은 ‘23. 1. 12. 기준으로 해지된 지 6개월이 지난 이용자의 개인정보를 고객인증시스템(CAS) DB 내 “ ” 테이블에 건, “ ” 테이블에 건을 파기하지 않고 보관하고 있었으며, 고객인증시스템(CAS) 개발기·검수기에는 ’08. 1월 이후 생성된 약 1,030만 건의 개인정보를 파기하지 않고 보관한 사실이 있다.

* 을 고객인증시스템(CAS) 개발기 DB 작업파일에, 고객정보을 CAS 검수기 DB 작업파일에 보관

나. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 고객인증시스템(CAS)의 웹서비스를 개발기는 ’07. 5월, 검수기는 ‘12. 8월, 운영기는 ’09. 12월부터 운영한 사실이 있으나, 개발기·검수기는 웹방화벽을 설치하지 않았고, 운영기에 설치된 웹방화벽은 ‘17. 4. 3. 이후 웹셸 등 불법적인 침입을 탐지하는 패턴 등 정책 업데이트 없이 운영한 사실이 있으며, 고객인증시스템(CAS) 개발기의 침입방지시스템(IPS)은 ’17. 3. 21. 이후 조사 시점인 ‘23. 1월까지 웹셸 등 불법적인 침입을 탐지하는 패턴 등 정책 업데이트 없이 운영한 사실이 있다.

개발자 등의 요청(‘15. 6. 3., ’16. 4. 19., ‘22. 7. 27. 등)에 따라 일시적으로 외부 특정 IP 주소에서 고객인증시스템(CAS) 개발기로 접근을 허용하는 정책을 개발기 방화벽에 등록하면서 요청 내역과 달리 모든 외부 IP(Any)에서 특정 포트(총 4개 포트)로 접속이 가능하도록 방화벽 정책을 등록하였고, 작업 종료 후에도 해당 정책을 만료하지 않고 ’23. 1월 조사 시점까지 허용상태를 유지한 사실이 있다.

피심인은 외부에서 접근 가능한 웹 서비스를 운영하면서 웹 관리자 계정 비밀번호로 초기 비밀번호를 이용(’09. 8. 5. ~ ’18. 7. 23.까지 제조사의 기본계정과 초기 비밀번호

를 이용)하고, 개발기의 DB 비밀번호를 반기별 1회 등 주기적으로 변경하지 않고 동일하게 사용한 사실이 있다. 또, 피심인은 개발기 서버에 '05. 12월 ~ '23. 2월 기간 동안 DB 계정정보 및 비밀번호를 평문형태로 7,485회 저장한 사실이 있으며, 검수기 서버에 '11. 3월 ~ '22. 7월 기간 동안 DB 계정정보 및 비밀번호를 평문형태로 579회 저장한 사실이 있다.

피심인은 개인정보취급자가 기한이 만료된 접근권한('18. 1. 31. ~ '19. 12. 31. 개발기로 SSH, FTP, SFTP 프로토콜을 이용해 접근할 수 있는 권한을 부여받은 자가 '18. 4. 3., '18. 4. 6. TELNET을 이용해 접속한 업무로그가 확인됨)을 사용한 작업 기록이 있으나, 접근권한 없이 접속한 작업 기록을 확인·감독하지 않은 사실이 있다. 또한, DB 접근제어 장비를 개발기·검수기·운영기에 모두 설치하여 운영 중이나, DB 서버에 직접 접속하거나 서버 간 접속방식으로 개인정보를 조회하거나 다운로드하는 경우에는 조회한 내용, 조회한 건수, 다운로드 여부 등 개인정보취급자가 수행한 업무 내역이 남지 않게 접속기록을 저장하고 관리한 사실이 있다. 피심인은 DB 접근제어 장비가 아니라 서버 접근제어 시스템을 통해 작업자가 수행한 명령어를 기록으로 남기고 있어 확인 가능하다고 소명하였으나, 명령어 기록에는 개인정보취급자가 DB를 조회한 내용, 조회 건수, 다운로드 여부 등 자세한 정보를 확인할 수 없었다.

다. 개인정보 유출 신고·통지를 소홀히 한 행위

피심인은 유출 사실을 인지('23. 1. 2.)하고 '23. 1. 3.과 '23. 1. 5.에 유출 신고한 이후, 개인정보가 유출된 이용자 중 '23. 1. 10. 현재까지 서비스를 이용 중인 이용자에게 유출 통지(187,374건)한 사실이 있다. 그러나, 해커가 공개한 이용자 정보를 고객인증시스템(CAS) DB 및 해지 이용자 DB와 비교·분석하는 작업을 지연하여 유출된 데이터에 포함된 해지 이용자에 대한 유출 통지는 '23. 2. 3.에 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '23. 6. 19. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '23. 7. 3. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제21조제1항은 "개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다."라고 규정하고 있다.

나. 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 제48조의2제1항제2호는 "개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 이 조에서 '개인정보처리시스템'이라 한다)에 대한 접근 권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행"(가목) "개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영"(나목), "비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영"(라목), "그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)" 등을 하여야 한다고 규정하고 있다.

같은 법 시행령 제48조의2제1항제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등을 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제1항제4호는 “비밀번호의 일방향 암호화 저장(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2021-3호, 이하 ‘고시’) 제4조제1항은 “정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.”라고 규정하고 있고, 제4조제2항은 “정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.”라고 규정하고 있으며, 제4조제3항은 “정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.”라고 규정하고 있다.

제4조제5항은 “정보통신서비스 제공자등은 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 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있으며,

제4조제8항은 “정보통신서비스 제공자등은 개인정보취급자를 대상으로 ‘영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을

조합하여 최소 8자리 이상의 길이로 구성(1호)', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고(2호)', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경(3호)' 등의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다."라고 규정하고 있다.

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 있으며,

제5조제2항은 "단, 제1항의 규정에도 불구하고「전기통신사업법」제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야 할 최소 기간을 2년으로 한다."라고 규정하고 있다.

제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

고시 해설서는 고시 제4조제1항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 열람, 수정, 다운로드 등 접근권한을 부여할 때는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화하여 부여하여야 한다고 해설하고 있으며, 제4조제3항에 대해서는 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 5년간 보관하여야 한다고 해설하고 있다.

제4조제5항에 대해서는 정보통신서비스 제공자등은 불법적인 접근 및 침해사고 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있고, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 한다고 해설하고 있으며, 접근 제한

기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영(신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리하는 것) 및 이상 행위 대응(모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하는 것), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단하는 것) 등을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있다. 또한, IP주소 등에는 IP주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)을 포함한다고 해설하고 있다.

제5조제1항에 관하여는 정보통신서비스 제공자 등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 하며, 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인 등을 위해 식별자, 접속일시, 접속지, 수행업무(개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위) 등을 포함하는 접속기록을 최소 1년 이상 보존·관리해야한다고 해설하고 있으며, 기간통신사업자의 경우에는 대규모의 이용자 개인정보를 처리하고 개인정보 유출 등으로 인한 피해 가능성이 매우 높은 특수성 등으로 인하여 최소 2년 이상 접속기록을 보존·관리하여야 한다고 해설하고 있다.

제6조제1항에 관하여는 정보통신서비스 제공자등이 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 보조저장매체 등에 일방향 암호화(해쉬함수 적용)하여 저장하여야 한다고 해설하고 있으며, 비밀번호를 암호화 할 때에는 국내·외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호 알고리즘으로 암호화하여 저장하도록 한다고 해설하고 있다.

다. 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.”라고 규정하고 있다.

2. 위법성 판단

가. 불필요하게 된 개인정보를 파기하지 않은 행위

[보호법 제21조(개인정보의 파기)제1항]

피심인이 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었으나 지체 없이 파기하지 않은 행위는 보호법 제21조제1항을 위반한 것이다.

나. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 개인정보취급자에게 개인정보처리시스템에 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화하여 부여한 접근권한에 대한 관리가 소홀하여, 피심인이 관리하는 접근권한 내역에서는 부여하지 않았거나 권한이 만료된 것으로 기록된 접근권한을 사용하여 개인정보취급자가 개인정보처리시스템에서 개인정보를 처리한 것은 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제3항을 위반한 것이다.

피심인이 개발자의 요청과는 달리 고객인증시스템(CAS) 개발기로 접근을 허용하는 정책을 개발기 방화벽에 등록하면서 요청 내역과 달리 모든 외부 IP(Any)에서 접속이 가능하도록 운영하였고, 요청 작업이 종료된 이후 ‘23. 1월 조사 당시까지 해당 정책을 비활성화하지 않고 유효한 상태로 유지한 사실과, 고객인증시스템(CAS) 개발기의 침입방지시스템(IPS)에 ’17.3.21. 이후 ‘23. 1월 조사 당시까지 웹셸 등 불법적인 침입을 탐지하는 정책 업데이트가 없었고, 개인정보처리시스템인 개발기·검수기도 웹서비스를 운영하면서 웹방화벽을 설치하지 않고 운영한 사실과 운영기에 설치된 웹방화벽은 ‘17.4.3. 이후 ’23. 1월 조사 당시까지 웹셸 등 불법적인 침입을 탐지하는 정책 업데이트 없이 운영한 사실은,

피심인이 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영(신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리하는 것) 및 이상 행위 대응(모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하는 것), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단하는 것) 등을 활용하여 불법적인 접근 및 침해사고 방지를 위한 시스템을 체계적으로 운영·관리하였다고 볼 수 없으며, 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하거나, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템의 설치·운영을 소홀히 한 것으로 판단되며, 이는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제4항제5호를 위반한 것이다.

피심인이 개인정보처리시스템의 관리자 계정으로 누구나 알 수 있는 기본계정과 초기 비밀번호를 사용하였고, DB 비밀번호를 반기별 1회 이상 변경하지 않고 동일하게 사용한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제8항를 위반한 것이며,

비밀번호를 안전한 암호화 알고리즘으로 일방향 암호화하여 저장하지 않는 등 비밀번호 관리를 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제1항을 위반한 것이다.

피심인은 대규모 개인정보 추출 작업이 존재함에도 월 1회 이상 정기적으로 접속 기록을 확인·감독하지 않아 과도한 개인정보 다운로드 등 비정상 행위 탐지 및 대응조치가 적절히 이루어지지 않았고, 전기통신사업법 제5조의 규정에 따른 기간통신사업자임에도 개인정보취급자가 개인정보처리시스템에 접속한 접근 내역(식별자, 접속일시, 접속지 정보 등)과 수행한 업무(개인정보 입·출력 및 수정사항, 파일별·담당자별 데이터 접근 내역 등 처리한 내용) 등을 최소 2년 이상 보존·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항과 제2항을 위반한 것이다.

다. 개인정보 유출통지 및 유출신고를 소홀히 한 행위

[보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항]

피심인이 '23. 1. 5.에 유출 신고한 데이터 중 현재 이용자에 대해서는 '23. 1. 10.에 유출 통지했음에도 불구하고 유출된 정보에 해지 이용자가 있는지에 대한 확인을 지연하고 정당한 이유 없이 24시간을 초과하여 '23. 2. 3.에서야 유출 통지한 행위는 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보의 파기 위반	보호법 §21①		• 불필요하게 된 개인정보를 파기하지 않은 행위
안전조치의무 위반 (접근통제)	보호법 §29	§48의2① 제2호	• 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위(고시§4③,⑤,⑧)

			• 개인정보처리시스템에 대한 접속기록 보존·관리(고시§5①,②) • 개인정보의 암호화(고시§6①)
개인정보 유출 통지·신고 위반	보호법 §39조의4①	§48조의4	• 개인정보 유출통지 및 유출신고를 소홀히 한 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제39조의15제1항제5호, 같은 법 시행령 제48조의11제1항·제3항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 '개인정보보호 법규 위반에 대한 과징금 부과기준'(개인정보보호위원회 고시 제2022-3호, 이하 '과징금 부과기준')에 따라 과징금을 부과한다.

보호법 제39조의15제1항제5호에서는 '이용자의 개인정보를 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우'에 정보통신서비스 제공자등에게 과징금을 부과할 수 있다고 규정하고 있다. 또한, 민관합동조사단과 개인정보보호위원회 조사 결과, 유출된 개인정보의 출처로 고객인증시스템(CAS)의 DB가 확인되었고, 고객인증시스템(CAS)에서 ①웹방화벽, 침입방지시스템(IPS) 등 기본적 보안장비의 미설치 내지 설치 중이더라도 보안정책 적용 미흡, ②웹서비스 관리자 계정의 비밀번호를 누구나 알 수 있는 초기 비밀번호(jeusadmin)로 약 9년간('09.8.5 ~ '18.7.23) 그대로 운영, ③취급자에 대한 접근권한 관리 및 접속기록 확인·관리 소홀 등과 함께 조사과정에서 발견된 고객인증시스템(CAS)의 전반적인 관리 부실과 타사 대비 현저히 저조한 정보 보호·보안 관련 투자와 노력 부족이 금번 개인정보 유출 사고로 이어졌다고 보는 것이 합당하다. 이와 같이, 피심인은 보호법이 규정

하고 있는 기본적인 안전조치 의무를 준수하지 않은 상황에서 유출이 발생하였고, 대규모 이용자의 개인정보를 처리하고 개인정보의 유출이 일어났을 때 이로 인한 피해 가능성이 매우 높은 기간통신사업자로서 사회적으로 기대 가능한 책임을 온전히 이행했다고 볼 수 없어 과징금 부과가 불가피하다.

이에 따라, 다음과 같이 과징금을 부과한다.

가. 과징금 상한액

피심인의 위반행위에 대한 과징금 상한액은 같은 법 제39조의15제1항, 같은 법 시행령 제48조의11제1항에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액(다만, 해당 사업연도 첫날 현재 사업을 개시한지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액)의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은, 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 같은 법 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

피심인은 영리를 목적으로 정보통신망을 통해 정보통신서비스를 제공하는 자이며 보호법 시행령 제48조의2에 따른 안전성 확보조치를 이행하지 않은 사실이 있으므로 같은 법 제29조의 안전조치의무를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당하는 경우 '보통 위반행위'로, 1개 이상 2개 이하에 해당하는 경우 '중대한 위반행위'로 규정하고 있다.

피심인의 경우 위반행위로 인해 직접적으로 이득을 취하지 않은 경우, 위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우에 해당하여 '중대한 위반행위'로 감경한다.

3) 기준금액 산출

과징금 부과기준 제4조제1항에 따르면 관련 매출액은 위반 정보통신서비스 제공자등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다고 규정하고 있으며, 제2항에서는 제1항에 따른 관련 매출액 산정 시 서비스 범위는 전기통신사업법 제5조를 기준으로, ①서비스 제공 방식, ②서비스 가입 방법, ③이용약관에서 규정한 서비스 범위, ④개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식 등을 종합적으로 고려하도록 규정되어 있다. 전기통신사업법 제5조(전기통신사업의 구분 등)제1항은 전기통신사업은 기간통신사업 및 부가통신사업으로 구분한다고 규정하고 있으며, 제2항은 기간통신사업은 전기통신회선설비를 설치하거나 이용하여 기간통신역무를 제공하는 사업으로 한다고 규정하고 있으며, 부가통신사업은 부가통신역무를 제공하는 사업으로 한다고 규정하고 있다.

‘과징금 부과기준’ 제7조(위반기간의 산정)제1항은 같은 고시 “제6조제1항에 따른 위반기간은 위반행위의 개시일부터 종료일까지의 기간을 말한다. 다만, 위반행위가 과징금 부과처분을 명하는 개인정보보호위원회(이하 "보호위원회"라 한다)의 심의종결일까지 종료되지 아니한 경우에는 해당 사건에 대한 보호위원회의 심의종결일을 위반행위의 종료일로 본다.”라고 규정하고 있다.

피심인은 보호법 제29조(안전조치 의무) 위반사항과 관련하여 외부 IP 주소에서 고객인증시스템(CAS) 개발기로 접근허용 정책을 고객인증시스템(CAS) 개발기 방화벽에 등록하면서 요청 내역과 달리 모든 외부IP(Any)에서 접속이 가능하도록 등록하였고, 작업 종료 후 ‘23. 1월 조사 시점까지도 해당 정책을 만료하지 않는 등 외부 IP주소에 대한 접근통제가 미흡한 사실과 고객인증시스템(CAS) 개발기의 침입방지시스템(IPS)은 ’17. 3. 21. 이후 웹셸 등 불법적인 침입을 탐지하는 정책 업데이트가 없었고, 고객인증시스템(CAS) 개발기·검수기에 웹서비스를 운영하면서 웹방화벽을 설치하지 않았으며, 운영기에 설치된 웹방화벽은 ‘17. 4. 3. 이후 웹셸 등 불법적인 침입을 탐지하는 정책 업데이트가 없는 등 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 시스템 설치·운영을 소홀히 한 사실과 DB 서버에 직접 접속하거나 서버 간 접속방식으로 개인정보를 조회하거나 다운로드 등을 실행하는 경우에는 수행한 업무 내역이 남지 않게 접속기록을 저장·관리한 사실이 ’23. 1월 조사 시점까지 발견되었다. 따라서, ‘과징금 부과기준’ 제7조(위반기간의 산정)제1항에 따라, 피심인의 위반행위의 종료일은 보호위원회의 심의종결일이며, 과징금 부과를 위한 관련 매출액의 직전 3개 사업년도는 ‘20년, ’21년, ‘22년에 해당한다.

또한, 피심인의 이용자 정보가 유출된 시스템은 고객인증시스템(CAS)으로, 고객인증시스템(CAS)은 부가서비스의 가입·해지 등을 위한 시스템이며, 고객인증스템(CAS)에 대한 안전조치 의무 위반사항을 확인였고, 부가서비스 가입 방법, 이용약관, 시스템 관리 조직·인력 및 시스템 운영 방식이 별도로 존재하는

점 등을 고려하여, 피심인이 고객인증시스템(CAS)과 관련한 부가서비스 운영을 통해 발생한 매출액을 위반행위 관련 매출액으로 하고, 직전 3개 사업년도('20~'22년)의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2020년	2021년	2022년	평 균
관련 매출액				

※ 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	**1천분의 21**
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 피심인의 위반행위의 기간이 2년을 초과(고객인증시스템(CAS) 개발기 IPS는 '17.3.21. 이후 불법적인 침입을 탐지하는 정책 업데이트가 없음, 운영기에 설치된 웹방화벽은 '17.4.3. 이후 불법적인 침입을 탐지하는 정책 업데이트가 없음, '15.6.3., '16.4.19. 요청된 작업에 대해 요청 내역과 달리 모든 외부IP(Any)에서 접속이 가능하도록 등록한 후 작업 종료 후에도 '23.1월까지 허용상태 유지, '05. 12.월부터 '23. 1월까지 개발기 서버에 DB 계정정보 및 비밀번호를 평문 저장, '11. 3.월부터 '22. 7월까지 검수기 서버에 DB 계정정보 및 비밀번호를 평문 저장 등)하므로 기준금액의 100분의 50인 천원을 가중하고, 최근 3년 이내 법 제39조의15제1항 각 호에 해당하는 행위로 1회 이상의 과징금 처분을 받은 경우가 있으므로 가중한 금액을 유지한다.

* 피심인은 '20. 12. 9. 정보통신망법 제25조(개인정보의 처리위탁)에 따라 만원을 처분 받은 사실이 있다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

피심인은 ▲개인정보 보호를 위해 보호위원회가 인정하는 인증을 받은 점, ▲조사에 적극적으로 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 30에 해당하는 천원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 같은 법 시행령 제48조의11제1항·제4항, [별표 1의5] 2. 가. 1) (과징금의 산정기준과 산정절차) 및 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 6,800,452천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

위반행위	기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
안전조치 의무	천원	필수적 가중 (50% : 천원) 가중한 금액 유지 (1회 이상 위반)	추가적 가중 없음 추가적 감경 (30%, 천원)	6,800,452천원
		→ 천원	→ 천원	

2. 과태료 부과

피심인의 보호법 제21조(개인정보의 파기)제1항, 제29조(안전조치의무) 및 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제75조(과태료) 제75조제2항제4호·제6호·제12호의3 및 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(이하 '과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 있으므로 각 위반행위에 대해 위반횟수에 해당하는 과태료를 각각 적용한다.

< 피심인의 최근 3년간 처분내역 >

처분일시	위반내용	근거법령	처분내용	비고
'20.12. 9.	수탁자 관리·감독 및 시스템 접근통제 소홀	정보통신망법 제25조 (개인정보의 처리위탁) **제28조제1항** (개인정보 보호조치)	과태료 1,000만원	시정명령, 결과공표
'21. 5.12.	개인정보 미파기	**보호법 제21조1항** (개인정보의 파기)	과태료 360만원	
'22. 9.28.	해킹으로 인한 임직원 개인정보 29,546건 유출	**보호법 제29조** (안전조치 의무)	과태료 600만원	결과공표
'22.11.30.	시스템 접근통제 소홀	**보호법 제29조** (안전조치 의무)	과태료 1,200만원	결과공표

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
마. 법 **제21조제1항**·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)**을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우**	법 제75조 제2항제4호	600	1,200	2,400
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항을 위반**하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 **24시간을 경과하여 통지 또는 신고한 경우**	법 제75조 제2항 제12호의3	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

과태료 부과지침 제8조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 '안전성 확보에 필요한 조치를 하지 않은 행위'에 대하여 과태료 부과지침 제8조(과태료 가중기준) 및 〔별표2〕'과태료의 가중기준' 중 ▲제3호 위반행위별 각목의 세부기준에서 정한 행위가 2개인 경우에 해당하며(보호법 시행령 제48조의2제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 조치를 하지 않은 경우, 같은 법 시행령 제48조의2제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우 등), ▲법 위반상태의 기간이 3개월 이상인 경우로 기준금액의 20%를 가중하며, "불필요하게 된 개인정보를 파기하지 않은 행위'에 대하여 ▲법 위반상태의 기간이 3개월 이상인 경우로 기준금액의 10%를 가중한다.

2) **과태료의 감경**

과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우 과태료 부과기준 제7조(과태료 감경기준)에 따라 ▲과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료하거나, 시정 중에 있는 것으로 인정되는 점, ▲조사에 적극 협력한 점을 고려하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제21조제1항, 제29조, 제39조의4제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 2,700만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보의 파기 위반	1,200만원	120만원	600만원	**720만원**
안전조치의무 위반 (접근통제)	2,400만원	480만원	1,200만원	**1,680만원**
개인정보 유출등의 통지·신고에 대한 특례	600만원	-	300만원	**300만원**
계				**2,700만원**

3. 시정조치 명령

1. 피심인 ㈜엘지유플러스에 대하여 다음과 같이 시정조치를 명한다.

가. 운영 중인 개인정보처리시스템 전반에 대해「개인정보 보호법」제29조(안전조치 의무), 같은 법 시행령 제48조의2(개인정보의 안전성 확보조치)를 준수하고 취약 부분을 개선할 것

나. 전사적 차원에서 개인정보 내부관리계획(거버넌스)을 재정립(권한·책임 명확화)할 것

다. 개인정보 보호책임자의 역할과 위상(CEO 직속 조직구성 등) 및 전문성을 강화 할 것

라. 전 직원을 대상으로 정기적인 개인정보 보호 교육 계획을 수립하고 실시할 것

마. 개인정보처리시스템 내에 법령상 보관 의무가 없거나 처리 목적 달성 등으로 불필요하게 보관하고 있는 개인정보를 모두 파기할 것

바. 피심인은 가.부터 마.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 90일 이내에 이행결과를 개인정보보호위원회에 제출할 것

4. 결과 공표

「개인정보 보호법」 제66조제1항 및「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는

‘법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)’ 및 ‘위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)’에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 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	㈜엘지 유플러스	법 제21조	개인정보의 파기 위반	2023. 7. 12.	시정조치 명령 과태료 720만원
		법 제29조	안전조치의무 위반 (접근통제)		시정조치 명령 과태료 1,680만원
		법 제39조의4	개인정보 유출 등의 통지.신고에 대한 특례 위반		과태료 300만원

2023년 0월 00일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 보호법 제21조(개인정보의 파기)제1항, 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대하여 같은 법 제39조의15조(과징금의 부과 등에 대한 특례)제1항·제5호, 제75조(과태료)제2항제4호·제6호·제12호의3, 제64조(시정조치 등)제1항 및 제66조(결과의 공표)제1항에 따라 시정조치, 과징금, 과태료, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

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

피심인은 이 과징금 부과처분에 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.

2023년 7월 12일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)