개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2024 - 008 - 182호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (주)골프존 (사업자등록번호 :)

대표자

의결연월일 2024. 5. 8.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 7,504,000,000원

나. 과 태 료 : 5,400,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 회사 내 처리되는 개인정보 처리 흐름을 면밀히 분석하여 내부 관리계획을 재정립하고, 공유설정 등을 통해 개인정보가 유출되지 않도록 조치하는 등 제반 안전조치의무를 준수하는 한편 피심인이 관리하는 개인정보가 안전하게 처리될 수 있도록 개인정보 보호책임자의 위상과 역할을 강화할 것

나. 전 직원을 대상으로 개인정보 보호 교육을 주기적으로 실시할 것

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

3. 피심인의 법 위반 내용 및 처분 결과를 피심인 홈페이지에 공표명령한다.

가. 피심인은 처분 등에 대한 통지를 받은 날부터 1개월 이내 당해 처분 등을 받은 사실 등을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 2분의1 크기로 10일 이상 기간 동안(휴업일 포함) 게시할 것

나. 피심인은 원칙적으로 표준 공표 문안을 따르되, 공표 문안에 관하여 개인정보보호위원회와 미리 문서로 협의해야 하고, 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 개인정보보호위원회와 협의하여 정할 것

이 유

Ⅰ. 기초 사실

피심인은 정보주체에게 재화 또는 서비스를 제공하면서 개인정보를 처리하는 「개인정보 보호법」[1](이하 '보호법')상의 개인정보처리자로서 일반현황 및 최근 3년간 재무현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주 소	종업원 수(명)
㈜골프존				

< 최근 3년간 재무현황 > (단위 : 천원)

구 분	2020년	2021년	2022년	평균

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회(이하 '위원회')는 2023년 12월 12일 피심인이 개인정보 포털(privacy.go.kr)에 개인정보가 유출되었다고 신고함에 따라 개인정보 유출 관련 사실관계 및 보호법 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

1) 개인정보 보호법(법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행)

2. 행위 사실

가. 개인정보 수집 현황

피심인은 정보주체의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구 분	항 목	기 간	건 수(건)

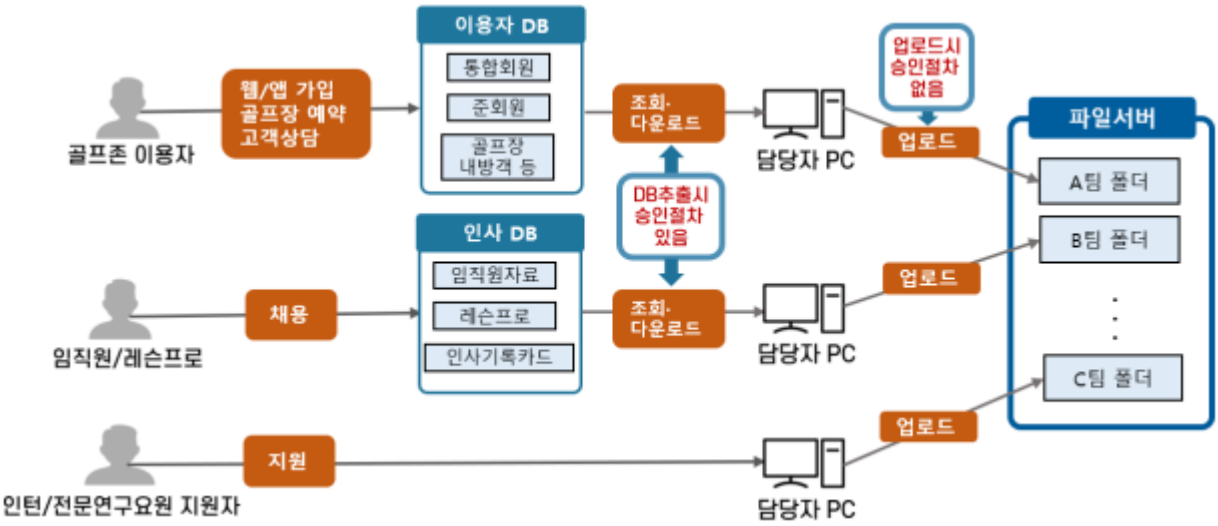
나. 피심인의 업무 형태

피심인은 임직원이 자료를 공유 및 보관할 수 있도록 윈도우 공유폴더 기능을 이용한 파일서버를 구축[2]하여 2024년 2월 16일까지 운영하였고, 임직원이 PC에 로그인하는 경우 파일서버의 저장공간(공유폴더)이 PC에 자동으로 연결되도록 구성하였으며, 일반 임직원은 자신이 소속된 조직(부서)의 폴더 또는 공용으로 사용하는 폴더에만 접근이 가능하였다.

파일서버는 모든 부서에서 전 임직원이 이용하고 있었고, 피심인의 각 업무 부서 또는 업무 담당자는 [3]에 따라 데이터베이스(개인정보처리 시스템, 이하 'DB') 내 개인정보 등을 추출·수령하거나, 정보주체로부터 직접 개인정보를 수집하여 이를 파일화한 후 파일서버에 업로드하여 저장·관리하고 있었다.

2) 파일서버 최초 도입일은 확인할 수 없으나, '17.7.14. 서버를 초기화하여 새롭게 구축함
3)

유출된 개인정보 파일 관련 부서(8개)	파일서버 이용자
	전 직원



참고로 피심인은 시스템[4]망을 구축·운용하고 청담·대전 사업장에 업무망을 구축·운용하였으며, 업무망에는 임직원의 업무용 PC가 존재하는 오피스존과 사용자 인증 및 권한부여 관리서버(이하, 'AD 서버') 및 파일서버 등이 존재하는 서버존을 구분하여 운용하고 있는데, DB의 개인정보 유출 등은 확인되지 않았다.

다. 개인정보 유출 관련 사실관계

1) 유출 경위

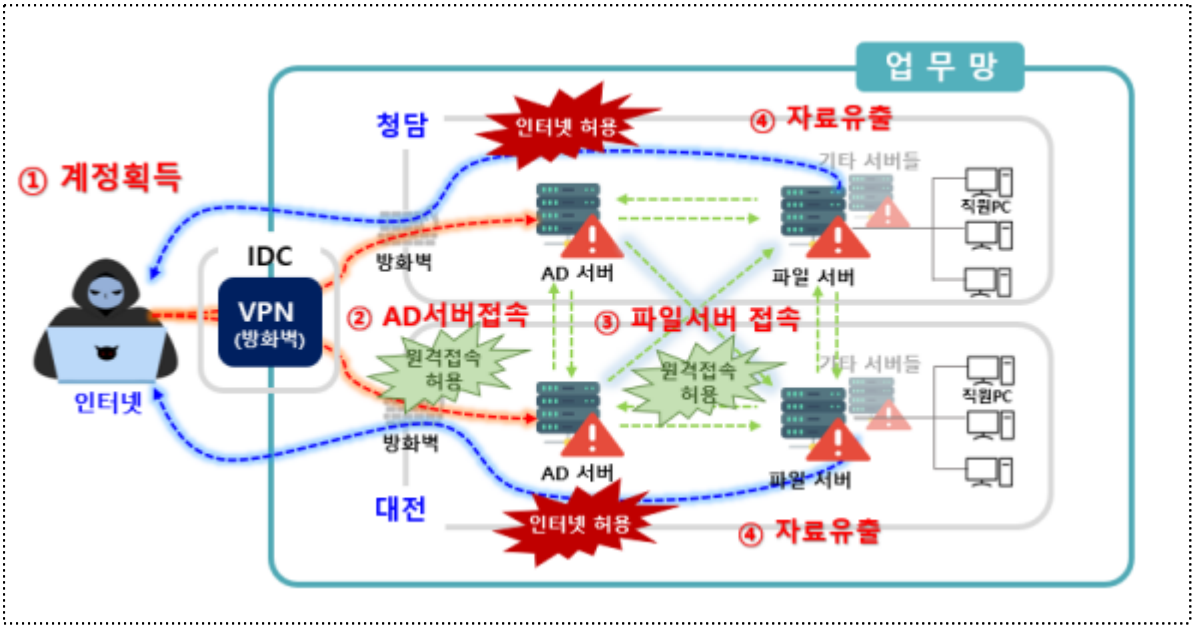
신원 미상의 자(이하 '해커')는 미상의 방법으로 피심인 직원들의 가상사설망(이하, 'VPN') 계정 및 비밀번호를 획득하였으며, 이 계정 중에는 파일서버 및 AD 서버의 관리자 권한이 부여된 계정(이하 '관리자 계정')도 포함되어 있었다.

4) 개인정보처리시스템(웹/앱 이용자 개인정보), 서버, VPN 장비 등이 보관됨

해커는 탈취한 관리자 계정으로 VPN에 로그인 후, 2023년 11월 22일 다른 네트워크(대전과 청담 사업장)에 존재하는 AD 서버에 각각 원격으로 접속하였고, AD 서버에서 대전과 청담 사업장의 파일서버에 각각 원격으로 접속하여 2024년 11월 22일부터 23일까지 각 파일서버의 자료들을 외부로 전송한 후 다크웹에 공개[5]하였다.

유출된 파일은 피심인의 파일서버에 업로드되어 있던 파일로 통합회원, 문화상품권, VOC, 인사 등 각 전용 DB로부터 추출된 개인정보와 담당자가 수집하여 업무 PC에 저장했던 개인정보가 파일화(xls, doc, pdf, csv 등)되어 저장·관리되고 있었다.

< 해커의 개인정보 유출 과정 및 문제점 >



2) 유출 규모 및 항목

2024년 2월 25일 기준 피심인이 보유한 개인정보 중 이용자, 임직원 등의 이름, 전화번호, 이메일, 생년월일, 아이디 등을 포함하여 최소 2,216,414건[6]의 개인정보가 유출되었고 이 중에는 일부 정보주체인 5,831명의 주민등록번호와 1,647명의 계좌번호도 포함되어 있었다.

5) 현재까지 확인된 유출 파일 용량 : 539GByte(압축파일, 압축 해제 시 1,180Gbyte)
다크웹에 공개된 파일은 파일서버에 저장되어 있었던 파일들의 일부인 것으로 확인되며 파일서버의 모든 파일이 유출된 건지 또는 해당 정보만 유출된 것인지는 확인되지 않음
6) 개인정보가 유출된 파일의 정보주체 수를 합산한 것으로 중복이 포함되어 있을 수 있음

유출된 개인정보 파일을 세부적으로 살펴보면 '준회원[7]' 이름, 전화번호와 '통합회원' 이름, 전화번호, 아이디, 회원번호가 유출되었고, 피심인의 고객센터로 문의한 이용자의 이름, 아이디, 전화번호, 계좌번호, 문의 내용 등 개인정보가 유출되었으며, 해당 문의 내역에는 비즈몰의 주문 취소 및 환불 등과 관련한 이용 문의가 포함되어 있다.

심지어, 유출된 파일 중 일부에는 주민등록번호도 포함되어 있었는데 'GDR 임직원 및 레슨프로, 사내 임직원·가족' 파일에서 , 'VOC 문의내역' 파일에서 , '인사기록카드 등 인사관련' 파일 등에서 주민등록번호가 유출되었다.

유출된 개인정보 파일별 유출 항목 및 규모[8]는 아래와 같다.

< 파일별 유출 항목 및 규모 >

연번	정보처리시스템 (DB, 담당자 PC 등)	개인정보 파일명	유출항목	유출규모 (주민번호)	파일 마지막 수정일
1					
2					
3					
4					
5					

7) 준회원 제도('20.6.2. 이후 신규 가입은 중단됨) : 스크린 연습장, 마켓 등 오프라인 매장에서 서비스 이용시 마일리지를 적립할 수 있는 바코드 발급을 위해 운용하던 제도로, 앱이나 홈페이지를 통해 가입하지 않은 비회원의 경우 개인정보 수집·이용 동의 후 바코드가 포함된 실물카드를 발급

8) 피심인이 다크웹에 유출된 파일을 개인정보 항목이 유사한 파일끼리 분류하여 제출한 자료
'파일 마지막 수정일'은 파일명에 날짜가 있거나, 파일 내용에 날짜가 있거나, 파일이 수정된 날짜가 있는 경우 중 가장 마지막 날짜 기준으로 작성됨

연번	정보처리시스템 (DB, 담당자 PC 등)	개인정보파일명	유출항목	유출규모 (주민번호)	파일 마지막 수정일
6					
7				( )	
8					
9				( )	
10				( )	
11				( )	
12					
13					
14				([9])	
15					
16					
17					
18				( )	
19					
20				( )	

9)

3) 유출 인지 및 대응

피심인은 2023년 12월 9일 한국인터넷진흥원(이하 'KISA')으로부터 골프존 데이터로 추정되는 파일이 다크웹에 공개되었다는 사실을 전달받았고, 다크웹에 접속하여 해당 파일에 대한 다운로드를 시작하였다.

2023년 12월 11일 피심인은 네트워크 불안정 등의 이유로 539GB 중 30GB 수준의 자료만을 다운로드하고 있는 상태에서 특정 보안업체[10]로부터 다크웹에 공개된 파일에 개인정보가 포함되어 있다는 연락을 받았고, 해당 보안업체와 미팅을 통해 해당 개인정보가 피심인으로부터 유출된 개인정보 중 일부임을 확인하였다.

피심인은 2023년 12월 12일 개인정보 보호 포털에 유출 신고를 접수하였고, 2023년 12월 14일 홈페이지에 안내문을 게시하였으며, 정보주체에게 유출 사실을 통지하기 시작하였다.[11]

< 피심인의 유출 인지·대응 >

일시		피심인의 유출 인지·대응 내용
'23.11.22.~23.		• 랜섬웨어 감염 및 개인정보 유출 사고 발생
'23.12.9.	08:53	• KISA를 통해(메일) 피심인의 데이터로 추정되는 파일이 다크웹에 공개되었다는 사실을 알고 해당 파일 다운로드 시작
'23.12.11.	11:05* * 메일 시스템 수신시각	• 보안업체( )로부터 다크웹에 공개된 정보에 개인정보가 포함되었다는 사실을 연락받음(메일, 유선) ※ 당시 피심인은 다크웹의 특성상 네트워크 불안정 등으로 30GB 수준의 자료를 다운로드하고 있는 상태였음
'23.12.12.	10:00~18:03	• 해당 보안업체와 미팅을 통해 유출된 개인정보 일부를 확인하고 개인정보 보호 포털에 유출 신고
'23.12.14.	11:53~	• 홈페이지 안내문 게시, 문자 등 유출통지(총 10회*) * 다크웹에 게시된 자료 전체에 대한 압축 해제 및 분석 후 유출된 정보주체가 확인될 때마다 통지

10)

11) 다크웹에 게시된 자료 전체에 대한 압축 해제(해제시 1,180Gbyte) 및 분석에 장시간이 소요되어, 유출된 정보주체가 확인될 때마다 통지하였다고 소명함(12월 14/15/16/17/18/19/20/21/22/29, 총 10회)

3. 안전조치의무 등 보호법 위반 관련 사실관계

피심인은 개인정보취급자를 포함하여 전 직원을 대상으로 파일 공유 등을 위한 파일서버를 운영하고 있음에도 가.파일서버 내 개인정보 파일 최소 1,288개 및 그에 포함된 221만 건 이상의 개인정보가 불필요하게 지속 공유되는 사실을 인지하지 못하고, 불필요한 원격접속과 인터넷 접속을 허용하는 등 유출방지 조치를 하지 않았으며 나.주민등록번호를 포함한 개인정보를 암호화하지 않고, 다.보유기간 경과, 목적 달성 등 불필요한 개인정보를 파기하지 않은 것으로 조사되었다.

가. 파일서버의 안전조치를 소홀히 하여 불필요한 공유설정과 광범위한 인터넷 접속을 허용한 행위

1) 파일서버에 대한 관리 부재

피심인은 파일서버를 개인정보취급자를 포함한 전 직원이 사용할 수 있도록 하였음에도 파일서버에 개인정보가 저장되어 공유되고 있다는 사실을 인지하지 못하였고, 이에 대한 관리체계도 미흡함에 따라 개인정보 파일 최소 1,288개 및 그에 포함된 221만 건 이상의 개인정보가 불필요하게 공유되고 있었으며 유출되지 않도록 필요한 조치를 하지 못하였다.

피심인의 내부관리계획 등에는 파일서버에 파일 업로드 시 개인정보를 탐지·차단하는 정책 또는 승인 절차, 파일서버에 업로드된 개인정보 파일에 대한 보관 기간 제한이나 삭제 기준, 암호화 여부 등에 대한 주기적 점검이나 불필요한 개인정보의 파기 절차 등 개인정보파일을 안전하게 공유·보관하는 것에 대한 정책이 확인되지 않으며, 심지어 피심인의 정보보안팀에게는 파일서버에 대한 점검 등 관리할 수 있는 권한조차 부여되지 않았다.[12)]

12) 파일서버의 관리 권한은 총 9명에게만 부여됨

이에, 엄격히 통제된 (인터넷망이 차단된 개인정보취급자의 PC 등 환경에서만 접속 가능한) DB에서 추출한 개인정보와 입회신청서 및 채용 관련 서류 등 담당자가 수집하여 PC에 저장한 개인정보 파일들도 파일서버에 업로드된 후 적절한 안전조치가 적용되지 않고, 파기 기한 없이 보관되었다.

2) 변화된 네트워크 환경에 대한 안전조치 부재

피심인은 기존에 외부에서 '그룹웨어 및 서버접속'을 위해 OTP 인증이 도입된 VPN[13]을 사용하고 있었는데, 코로나로 재택근무가 급격히 증가함에 따라 '그룹웨어 접속만을 목적'으로 하는 방화벽의 VPN 기능을 2020년 8월 24일 긴급히 활성화하였다.[14]

이 과정에서 VPN을 통해서는 외부에서 업무망으로 추가 인증 수단 없이 아이디, 비밀번호만으로 직접 접속이 허용되었고, 업무망 내 오피스존을 넘어 서버존까지도 접근[15]할 수 있게 되었다.

또한, 기존에는 외부에서 업무망의 서버존으로 원격접속이 허용되지 않았으나, 원격접속이 되도록 변화가 생겼고, 서버 관리자를 포함하여 모든 임직원에 대하여 VPN 계정에 대한 필요성 검토 및 별도의 신청 없이 VPN이 활성화되었으며, 하나의 계정(접근권한)으로 VPN, 업무용 PC 및 파일서버 등에 모두 접속이 가능한 상태가 되었다.

특히, 서버 간 원격접속 허용, 업무망의 서버존에 대한 인터넷 허용, 문서 DRM(암호화) 미적용 등 기존의 VPN 사용 시에는 드러나지 않던 보안 위험 요소가 드러나게 되는 등 침해사고의 위험성이 높아지게 되었다.

이와 같이 외부에서 내부 업무망에 접속할 수 있도록 VPN 기능을 도입·활성화하여 네트워크 보안 환경의 중대한 변화가 발생하였으나 피심인이

13) VPN은 그룹웨어 및 서버접속 등을 위해 사용하였고, 안전한 인증수단이 도입되어 있으며, VPN은 그룹웨어 접속만을 목적으로 하여 OTP 추가인증은 도입하지 않았다고 함

14) 기존 사용하던 VPN 라이선스 부족 문제가 발생하여 VPN을 긴급히 추가 도입함

15) VPN 계정은 전 직원의 계정이 별도 신청 없이 활성화되었는데, 서버 관리자도 권한 신청 없이 업무계정으로 AD서버 및 파일서버에 관리자로서 접근가능했음

VPN 도입 후 보안 위협요소, 각종 안전조치의 존재 및 필요 여부 등에 대하여 검토한 사실은 확인되지 않는다.

이에 개인정보 유출 사고가 발생하기까지 이러한 상태가 지속되었고 해커는 탈취한 관리자 계정으로 VPN을 통해 외부에서 업무망에 접속, 서버존에 있는 파일서버의 전체 폴더 및 파일에 접근한 후, 파일서버에서 바로 인터넷망에 접속하여 개인정보 파일을 외부로 유출하였다.

< >

❶

❷

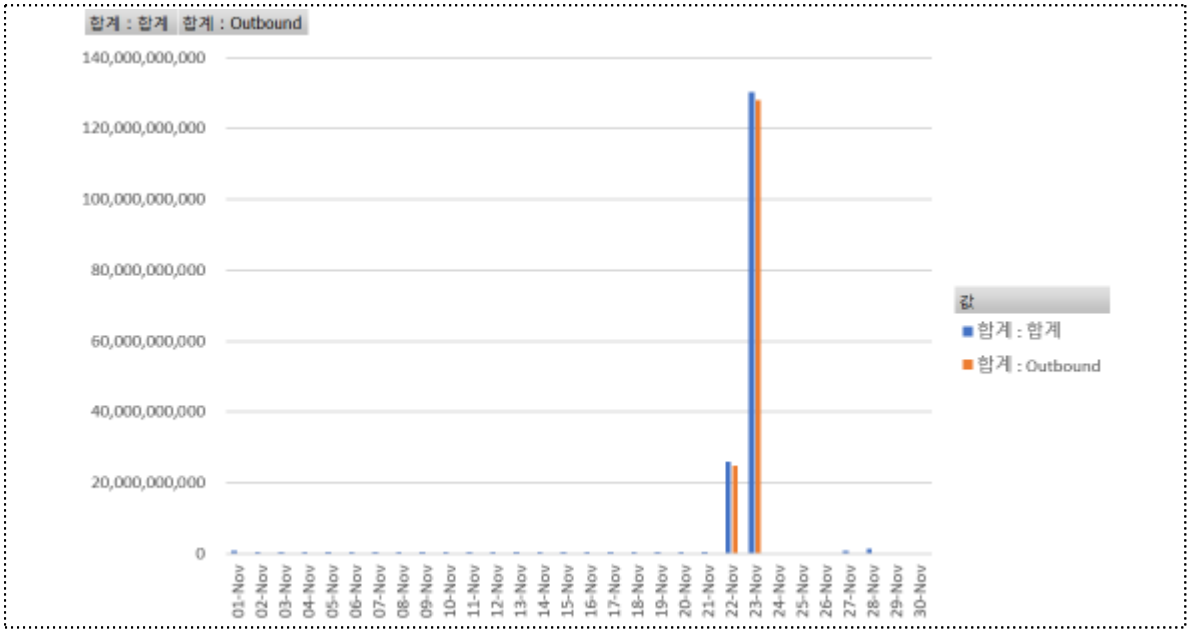
❸

❹

3) 개인정보 유출 사고 대응 지연

피심인은 2023년 11월 23일 파일서버의 랜섬웨어 감염 사실은 인지하였으나, 파일서버에 보관되고 있는 정보가 무엇인지, 개인정보가 포함되어 있는지를 전혀 인지하지 못하고 있었기 때문에 보안업체로부터 개인정보 유출 가능성에 대한 연락을 받은 2023년 12월 11일 전까지 파일서버에 대한 비정상적인 통신 여부 및 개인정보가 유출됐을 가능성에 대한 분석[16]은 전혀 없었고, 실제 랜섬웨어 감염 사고 후 개인정보 유출에 대한 이용자와 언론 등의 우려에도 불구하고 '회원 개인정보의 유출은 없다'고 밝혔다.

< 방화벽의 내→외부 전송 트래픽( )>



이에 피심인은 개인정보 유출이 발생한 후 20여 일이 지나서야 개인정보 포털에 신고를 접수하고, 정보주체에게 해당 사실을 통지하기 시작하였다.

4) 불필요한 원격접속 허용

피심인은 임직원의 업무용 PC뿐만 아니라 서버에서도 다른 서버에 대한 원격

16) 해킹이 특정 관리자 계정( )을 통해 발생한 사실을 확인하였음에도 해당 계정으로 발생한 통신 이력(파일서버 방화벽 로그) 등을 점검한 사실이 없음

접속이 가능하도록 관련 IP와 포트(Port)를 허용하였고, 다른 네트워크(청담·대전)에 존재하는 서버에도 이를 허용하고 있었다.

또한, AD 및 파일서버는 원격접속이 불필요함에도 방화벽의 VPN 기능을 통해 원격접속 하는 것을 허용하고 있었다.[17)]

이에 해커는 방화벽(VPN)에서 내부 AD 서버에 원격접속할 수 있었고, 다른 네트워크에 존재하는 파일서버에도 원격접속하여 개인정보 파일을 외부로 전송·유출할 수 있었다.

5) 불필요한 인터넷 통신 허용

통상의 기업들은 서버에 대해 외부로의 통신을 차단[18)]하도록 하고, 일부 서비스 제공과 관련된 경우에만 제한적으로 허용하며, 실제 피심인도 IDC 센터의 다른 서버들에 대해서는 방화벽 정책으로 외부로의 통신을 차단하고 있었다.[19)]

피심인은 업무망 내 오피스존과 서버존을 구분하지 않고 방화벽 정책을 적용·운용하면서 외부로 통신하는 경우 모든 네트워크 대역에서 인터넷 접속을 허용

17) VPN 기능 활성화 이전에는 외부에서 내부 AD서버 및 파일서버로 접속하는 경우 원격접속은 차단되어 있었으며, 피심인은 조사과정에서 AD와 파일서버에 대한 원격접속은 불필요했다고 인정함(원격접속은 제한된 환경(접근통제 솔루션, 관리자 PC 등)에서만 가능)

18) 네트워크 접근통제 정책 예시로, 서버망에서 인터넷망은 전체 차단하되, 필요한 ip와 포트에 대해서만 허용할 것을 보안강화 방안으로 명시(중소기업 서비스 개발 운영 환경 주요 보안 취약 사례별 대응방안('22.8월, KISA))

19) ISMS-P 인증기준(2.6.7 인터넷 접속 통제)은 불필요한 외부 인터넷 접속을 통제하도록 하고 있으며, DMZ 및 내부망에 위치한 일부 서버에서 불필요하게 인터넷으로의 직접 접속이 가능한 경우를 결함사례로 안내

하였고, 이에 청담·대전 업무망 내 업무용 PC 및 서버에 대해서는 그 필요성과 무관하게 모두 인터넷 접속이 가능하게 되었다.

이에 피심인의 AD 및 파일서버는 개인정보를 포함해 업무망 내에서 생성 및 처리되는 정보가 저장되고, 특히 인터넷 접속은 전혀 필요성이 없음[20]에도 불구하고 인터넷 접속이 가능하게 되었으며, 해커는 파일서버의 개인정보 파일을 바로 외부로 전송·유출할 수 있었다.

나. 주민등록번호를 포함한 개인정보를 암호화하지 않은 행위

피심인은 2021년 12월까지는 파일서버에 보관된 문서에 대해 문서보안 DRM 솔루션을 적용하여 암호화하고 있었으나, 기존에 사용하고 있던 DRM을 제품으로 교체하는 과정[21]에서 기존 DRM으로 암호화되었던 문서를 일괄 복호화한 후 이를 다시 암호화하지 않고 파일서버에 저장·보관하였다.

이에 따라 파일서버에 주민등록번호가 포함된 개인정보 파일과 이용자의 개인정보가 포함된 다수의 개인정보 파일이 전혀 암호화되지 않고 저장·보관되다가 그 상태로 해커에 의해 유출되었다.[22]

파일수[1]	파일유형(중복제거)[2]	주민번호 수[3]	주민번호 수(중복제거)[4]

20) 피심인은 조사과정에서 파일서버의 외부 인터넷 접속은 불필요했다고 인정하였으며, 업무망의 서버존에 대해 인터넷을 차단하는 조치를 취할 예정이라고 함

21)

22) 1) 주민등록번호가 포함된 파일(미암호화) 수치, 2) 유사파일을 중복 제거한 파일 수치
3) 이용자, 임직원의 주민등록번호 수치(13자리 평문), 4) 중복 제거한 주민등록번호 수치

다. 처리목적 달성 등 불필요한 개인정보를 파기하지 않은 행위

피심인의 파일서버에는 보유기간 경과, 개인정보 처리목적 달성 등 보유 근거가 없는 개인정보가 포함된 파일이 파기되지 않고 보관되고 있었다.

구체적으로 개인정보가 유출된 '준회원' 파일에서 현재 회원으로 확인되지 않는 정보주체는 , 임직원(레슨프로 포함) 정보 중 퇴사하여 보유 근거가 없는 정보를 파기하지 않았으며, 인턴사원, 전문연구요원 채용 등과 관련하여 수집한 정보주체 채용 관련 개인정보를 파기하지 않았다.

또한, VOC 관련 이용자 및 가맹점주 등의 주민등록번호를 포함한 개인정보도 세금계산서 발급, 제세공과금 신고 등 처리목적이 달성되었음에도 파기하지 않았다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2024년 3월 20일, 4월 5일 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2024년 4월 2일, 4월 18일에 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 관련 법규 및 위법성 판단

1. 관련법 규정

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

나. 보호법 제24조의2제2항은 “개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.”고 규정하고 있다.

다. 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[23](이하 ‘시행령’) 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’를 하여야 한다.”라고 규정하고 있으며, 제4호는 “개인정보를 안전하게 저장·전송하기 위해 ‘주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치(나목)’를 하여야 한다고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 개인정보의 안전성 확보조치 기준[24](이하 ‘안전성 확보조치 기준’) 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.”고 규정하고 있다.

안전성 확보조치 기준 제7조제5항은 “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.”고 규정하고 있다.

23) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
24) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

2. 위법성 판단

가. 불필요하게 된 개인정보를 파기하지 않은 사실

[보호법 제21조(개인정보의 파기)]

피심인이 파일서버에서 보유기간의 경과 및 개인정보의 처리목적 달성 등으로 불필요하게 된 개인정보를 파기하지 않은 행위는 보호법 제21조제1항 위반에 해당한다.

나. 주민등록번호를 암호화하여 보관하지 않은 사실

[보호법 제24조의2(주민등록번호 처리제한)]

피심인이 파일서버에 주민등록번호가 포함된 다수의 개인정보 파일을 보관하면서, 해당 정보가 유출되지 않도록 암호화 조치를 하지 않은 행위는 보호법 제24조의2 제2항 위반에 해당한다.

다. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 사실

[보호법 제29조(안전조치의무)]

안전성 확보조치 기준은 개인정보가 유출되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 하고 있고, 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하는 것을 원칙으로 정하고 있다.

피심인은 통합회원 정보를 관리하고 있고, ISMS 인증 의무대상[25] 이며, 다양한 경로로 개인정보를 처리하는 연 매출 5천억 원 대의 중견기업으로, 회사 전반의 개인정보 처리 흐름을 분석하고, 개인정보 유출에 영향을 미칠 수 있는 다양한 위험 요소를 통제하여 개인정보가 유출되지 않도록 조치할 필요가 있다.

25) 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간 일일평균 이용자수 100만명 이상에 해당

피심인은 파일서버에 대하여 개인정보취급자를 포함한 전체 임직원이 사용할 수 있도록 하였고, 개인정보 파일이 업로드되는 것을 기술적·관리적으로 제한하지 않았으며, 파일서버는 관리자가 권한을 부여받은 컴퓨터의 공유폴더 기능을 이용하여 각 부서 임직원들의 PC에 별도 폴더가 생성되어 공유되는 것이므로, 안전성 확보조치 기준 제6조제3항에 명시된 개인정보가 인터넷 홈페이지, P2P, '공유설정' 등을 통해 공개·유출 가능한 요인을 점검하고 이를 방지하기 위한 조치를 취해야 하는 '개인정보취급자의 컴퓨터 및 모바일 기기 등'에 해당한다.

그러나, 피심인은 파일서버에 221만 건 이상[26]이나 되는 대량의 개인정보가 저장되어 있음에도 파일서버에 저장·보관되고 있는 개인정보가 포함된 파일에 대한 암호화 여부 점검이나 주기적 파기 등에 대한 관리가 없었을 뿐만 아니라 파일서버 내 개인정보의 존재조차 알지 못하였다.

또한, 외부에서 내부 업무망에 접속할 수 있도록 VPN 기능을 도입·활성화하는 것은 네트워크 보안 환경의 중대한 변화가 발생한 것이므로, 이에 따른 침해사고 위험에 대해 지속적으로 검토하고 보완하는 것이 필요하나, 피심인은 코로나19로 인한 재택근무의 증가로 방화벽의 VPN 기능을 OTP 등 추가 인증 수단을 적용하지 않고 활성화하였음에도 개인정보 유출 사고가 발생하기 전까지 이로 인한 개인정보 침해 위협을 검토하고 보완조치를 하지 않았다.

이에 외부에서 업무망 내 오피스존의 PC 및 서버존의 파일서버 등에 아이디, 비밀번호만으로 직접 접속이 허용되었고, 서버 관리자는 파일서버에 별도 승인 없이 불필요한 원격접속을 할 수 있게 되었으며, VPN 계정 등이 필요성 검토 및 별도의 신청 없이도 활성화되고, 심지어 해당 계정으로 오피스존의 PC뿐만 아니라 서버존의 AD 서버 및 파일서버에도 접속이 가능하게 되었다.

아울러, 서버 간 원격접속 허용, 서버존에서의 인터넷 접속 허용 등 기존 피심인이 갖고 있던 보안 위협 요소도 드러나게 되었다.

---

26) 피심인의 통합회원 DB보유량이 이상이므로('24.2월 기준) 전체 개인정보 보유량의 %이상이 파일서버에 저장되어 있었음

이러한 사정으로 해커는 탈취한 VPN 계정을 통해 파일서버에서 공유·보관되는 개인정보 파일을 외부로 전송·유출할 수 있었고, 이는 대표적인 공유설정을 통한 개인정보 유출에 해당한다.

대법원은 舊 개인정보의 기술적·관리적 보호조치 기준[27](이하 '舊 기술적 보호조치 기준') 제4조제9항(現 고시 제6조제3항)은 내부적 부주의뿐만 아니라 외부로부터의 불법적인 접근(해킹 등)에 의한 개인정보 유출을 방지하기 위한 목적으로 마련되었다고 판단[28]하면서 제공자의 의무로 규정된 '조치'는 해킹 등에 의해 유출되지 않도록 '처리시스템과 취급자 PC 등'에 취하여야 할 사회통념상 합리적으로 기대 가능한 정도의 기술적 보호조치로 아래 판단기준을 제시한 바 있다.

(1) 해킹 등 침해사고 당시 일반적으로 알려져 있는 정보보안 기술 수준
(2) 정보통신서비스 제공자의 업종과 영업 규모
(3) 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용
(4) 정보보안조치에 필요한 경제적 비용 및 그 효용의 정도
(5) 해킹기술 수준과 정보보안기술 발전 정도에 따른 피해 발생 회피 가능성
(6) 정보통신서비스 제공자가 수집한 개인정보의 내용
(7) 개인정보 누출로 인하여 이용자가 입게 되는 피해 정도

「舊 개인정보의 기술적·관리적 보호조치 기준 개정 해설서」('22.8.)는 개인정보처리시스템, 컴퓨터, 모바일 기기 등에서 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요할 때에는 권한 설정 등의 조치를 하여야 한다고 명시하고 있다.

KISA가 발간한 「랜섬웨어 스페셜 리포트」(´21.9.), 「랜섬웨어 대응 가이드」(´23.8.)에서는 공유폴더 및 네트워크 드라이브에 대한 랜섬웨어 공격 사례 및 보안 위협 등을 설명하면서 공유폴더의 사용 및 외부 인터넷 사용 여부 등에 대한 보안성 주기적 점검, 사용 권한의 재평가 등 강력한 대응을 요구하고 있다.

27) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15.. 시행
28) 대법원 2021. 8. 19. 선고 2018두56404 판결

또한, 코로나를 계기로 전 세계의 기업들이 재택근무 체제로 전환하면서 원격접속(RDP)[29]을 이용한 해커의 공격(특히 랜섬웨어 공격)이 크게 증가하며 이에 대비한 보안 강화 필요성이 중요시되었던바, 피심인은 재택근무 확대로 VPN을 활성화하면서 이러한 해설서 및 안내서를 통해 원격접속을 통한 공격을 예측하고, 시스템별로 원격접속의 필요성을 검토하거나 파일서버 및 공유폴더에 대한 보안 위협을 검토하는 등 충분히 대비할 수 있었다.

< 舊 개인정보의 기술적·관리적 보호조치 기준 개정 해설서('22.8.)), p.57~58) >

▸ P2P 및 **공유설정을 통한 개인정보 유·노출 방지 조치**

- 개인정보처리시스템, 컴퓨터, 모바일 기기 등에서 P2P, **공유설정은 기본적으로 사용하지 않는 것이 원칙**이나, 업무상 반드시 필요할 때에는 권한 설정 등의 조치를 통해 **권한이 있는 자만 접근할 수 있도록 설정**하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 **접근 통제 등에 관한 보호조치**를 하여야 한다.

< 공유폴더 등에 대한 랜섬웨어 위험성 경고 >

▸ 「**랜섬웨어 스페셜 리포트**」('21.9., KISA) 운영자 PC에 대한 보안 강화

- 랜섬웨어 피해예방을 위해 **공유폴더 사용**, **외부 인터넷 사용 여부** 등에 대한 보안성을 주기적으로 점검해야 함

▸ 「**랜섬웨어 대응 가이드**」('23.8., KISA) 공격 제한 방법을 위한 접근통제

- 관리자의 경우 랜섬웨어 감염 시 확산되지 않도록 **공유 네트워크 드라이브에 대한 사용권한**을 정기적으로 재평가 할 것

< 비대면 업무환경 도입 운영을 위한 보안 가이드(과기부/KISA, '20.6.) >

▸ 기업망 모니터링 강화 체크리스트 中 "**불필요한 서버간 접근을 최소화** 하고 필요시 계정별 권한을 부여하는 접근통제를 적용하고 있는지 여부"를 확인

< RDP를 통한 해커 공격 증가 관련 통계 >

▸ '20년 한해 RDP공격이 안정적 성장률을 유지하고, **'21년 1분기에 비해 4분기에** 보고된 공격은 **총 768% 증가**함(보안업체 ESET 보고서)

▸ RDP공격 : '21.2월 9,310만회 → '21.3월 2억7,740만 회로 **197% 증가율**(보안업체 Kaspersky 보고서)

▸ '22~'23년 사이 자사의 공격 표면 관리 솔루션을 통해 수집한 데이터를 분석한 결과, 분석대상 조직의 85% 이상이 한달 중 최소 25%동안 RDP를 통해 인터넷에 접속하는 추이를 보였으며, **랜섬웨어 공격이나 무단 로그인 시도에 노출됨**(소프트웨어 업체 Palo Alto Networks 보고서)

29) Remote Desktop Protocol(원격 데스크톱 프로토콜) : 사무실 PC가 켜져 있는 경우, 이동 또는 재택근무 시에도 업무용 컴퓨터에 접근이 가능하도록 하는 기술

그리고 스크린골프 점유율 1위, 2022년 기준 연 매출 , 당기순이익 이상의 중견기업인 피심인은 코로나 당시 우선적으로 VPN만 긴급히 도입(활성화)할 수밖에 없었더라도[30], 이후 OTP 라이선스 등을 구매하여 안전한 인증수단 적용 등의 조치를 취할 수도 있었다.

보다 근본적으로는 네트워크 환경이 변화되었을 때, 침해사고 위험을 검토하여 파일서버에 대한 관리체계 구축, 업무망 내 서버존의 불필요한 인터넷 접속 차단, 이미 도입된 DRM을 활용한 파일 암호화 또는 불필요한 개인정보 파일 삭제 등의 조치를 통해 이 사건의 유출을 차단할 수 있었고, 이는 별도의 비용이 들지 않는다.

따라서 피심인이 공유설정을 통한 개인정보 유출 등을 방지하기 위해 어떠한 조치도 하지 않은 행위는 보호법 제29조 같은법 시행령 제30조제1항제3호, 안전성 확보조치 기준 제6조제3항 위반에 해당한다.

피심인이 이용자의 개인정보와 임직원 등 정보주체의 주민등록번호를 파일서버에 저장하면서 문서보안 DRM 솔루션 교체시 일괄 복호화된 파일을 재암호화 하지 않고 파일서버에 그대로 보관한 행위는 보호법 제29조, 같은법 시행령 제30조제1항 제4호, 안전성 확보조치 기준 제7조제5항 위반에 해당한다.

Ⅳ. 피심인의 주장에 대한 검토

1. 개인정보 유출 및 안전조치의무 위반에 대하여

가. 피심인 주장

피심인의 파일서버는 개인정보를 처리하기 위한 목적으로 구성된 시스템도 아니고 데이터베이스와 연동되어 있지 않으므로 고시상(제5조제1항, 제6조제1항제1호 및 제2호, 제6조제2항 등) 각종 안전성 확보조치 적용 대상이 되는 개인정보처리시스템에 해당하지 않는다고 주장한다.

---

30) VPN에는 안전한 인증수단이 도입되어 있으며, 에는 라이선스 구매가 필요하여 즉시 안전한 인증수단을 도입하지는 못하였다고 소명

또한, 보호법 시행령과 고시에서는 서버의 원격 접속 등 서버 간 통신 제한이나 외부방향 통신을 통제하는 조치를 취할 의무를 부과하고 있지 않고, 서버 간 원격 접속을 통한 시스템 관리는 흔하게 존재하며, 업무공간에서 외부 사이트 연결을 위한 외부방향 통신 허용 정책이 필요했다고 주장한다.

나. 검토의견 : 불수용

위원회는 피심인의 파일서버를 공유설정 등을 통해 공개·유출 가능한 요인을 점검하고 이를 방지하기 위한 조치를 취해야 하는 기기 등에 해당하는 것으로 보고, 이에 대한 어떠한 보호조치도 하지 않은 피심인이 고시 제6조제3항을 위반한 것으로 판단하였으며, 그 판단은 파일서버의 개인정보처리시스템 여부와 전혀 무관하다.

오히려, 피심인의 주장은 파일서버에 221만 명의 개인정보와 주민등록번호 등 중요 개인정보를 보관하고 있음에도 개인정보처리시스템인 경우 적용하여야 하는 안전조치를 적용하지 않았다는 것을 자인하는 것으로 볼 수 있다.

또한 피심인은 파일서버가 개인정보처리시스템임을 전제로 안전조치의무를 위반하지 않았다고 주장할 뿐, 개인정보처리시스템으로 보지 않은 경우에 대해서는 별도로 주장하고 있지 않다.[31)]

특히, 피심인은 공유설정과 관련한 보호조치에 대한 소명이나, 파일서버에 개인정보가 존재함을 인지하지 못해 주기적 관리나 암호화 등을 하지 않은 행위에 대해서는 의견을 제시하지 못하였다.[32)]

피심인이 파일서버를 구성하여 임직원이 업무 과정에서 처리하는 개인정보 파일을

31) 피심인은 심의·의결 당일 의견진술 과정에서 공유설정은 서버가 아니라 업무용 컴퓨터에 있는 파일을 공유폴더 설정 등을 통해 이용하는 상황을 전제하므로 고시 제6조제3항 위반은 인정될 수 없다고 주장하나, 피심인의 행위가 업무용 컴퓨터에 있는 파일들을 업무용 컴퓨터에 설정된 공유폴더에 저장·이용한 것임

32) 피심인은 심의·의결 당일 의견진술 과정에서 피심인은 직원이 소속 부서 폴더에만 접근할 수 있도록 권한을 제한하고 있었고, 부서이동 또는 퇴사시 권한 조정 및 삭제가 이루어졌다고 하였으나, 공유폴더를 통해 개인정보가 공유되는 상황, 외부로 유출되지 않도록 하는 조치에 대해서는 의견을 제시하지 못함

공유하면서 조회·변경·복사 등 할 수 있도록 운영한 것은 전형적인 공유설정에 해당하는바, 피심인은 안전조치 기준 제6조제3항에서 규정한 공유설정을 통한 유출 요인을 점검 및 조치해야 하고, 파일서버(공유폴더) 안의 개인정보 여부 파악 및 점검, 네트워크 및 업무 환경 변화에 따른 개인정보 유출 가능성 검토·차단, 불필요한 원격접속 차단과 외부 통신 제한 등은 해당 점검 및 조치에 포함된다고 판단된다.

또한, 피심인은 서버 간 원격접속이 흔하게 존재한다고 할 뿐, 원격접속이 필요한 사유는 주장하고 있지 않으며 외부에서 AD 및 파일서버에 대한 원격접속, AD 서버와 파일서버 간 원격접속의 불필요성에 대해서는 피심인이 이미 현장조사 과정에서 인정하여 사실확인서를 통해 최종적으로 확인하였다.

피심인은 대부분의 회사에서 업무공간의 인터넷 접속을 허용하고 있다고 주장하나, 피심인과 같이 업무공간에 서버존을 두고 인터넷 접속을 모두 허용하는 경우는 일반적이지 않고, 오히려 업무공간에서 다량의 개인정보를 처리하는 업무용 PC는 인터넷망을 차단[33]하고 있다.

실제 피심인 또한 AD 및 파일서버가 존재하는 내부 네트워크에서 외부로 통신하는 경우에도 필요한 IP, Port로만 통신을 제한하고 있지 않았다고 인정하면서, 사고 이후 서버존에 대한 인터넷을 차단하는 조치를 취할 예정이라고 한바, 피심인의 의견을 수용할 수 없다.

33) 특히, 안전성 확보조치 기준 제6조제6항은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대해 인터넷망 차단 조치를 규정

2. 과징금 산정에 대하여

가. 피심인 주장

피심인은 준회원과 통합회원의 개인정보 처리로 매출액이 발생하기 때문에 준회원 또는 통합회원의 개인정보 처리가 발생하는 매출액 외의 매출액을 전체 매출액에서 제외하여야 한다고 하면서, 스크린골프 사업자들에게 시뮬레이터를 판매하여 발생하는 매출은 사업자들로부터 발생하는 매출로 개인정보의 처리가 발생하지 않으며 서비스 이용이 아닌 기기의 판매에서 발생하는 매출이라는 점에서 제외되어야 한다고 주장한다.

또한, 시뮬레이터 운영에 따른 소모품인 골프매트, 고무티, 스크린 등 자재 및 시뮬레이터 이전 설치를 포함한 A/S서비스 제공 및 스크린골프장 관리 소프트웨어를 제공하여 발생한 기타 판매 매출, 시뮬레이터 및 스크린골프장 운영관리에 필요한 소모품을 온라인으로 판매하는 '비즈몰'도 일반 이용자 대상 서비스가 아니고 본 사고로 영향을 받지 않아 제외되어야 하며, 광고 및 제휴 매출과 기타 계열사 지원, 주니어 골프선수 육성 아카데미, 부동산 임대 매출 등으로 발생한 매출 역시 제외되어야 한다고 주장한다.

나. 검토의견 : 일부 수용

피심인이 국내에서 제공하는 스크린골프 서비스는 이용자들이 피심인의 웹사이트 또는 앱(Golfzon, GDR 등)을 통해 회원으로 가입하여 스크린골프장 등에서 시뮬레이터로 로그인한 후[34] 서비스를 이용하고, 시뮬레이터를 통해서 처리되는 경기 결과, 스윙 영상 등 서비스 이용 결과를 이용자가 다시 웹사이트 또는 앱에서 볼 수 있으므로, 시뮬레이터가 개인정보를 이용한 서비스와 별개의 것으로 보기 어렵다.

34) 피심인은 회원으로 가입하는 이유가 시뮬레이터 이용에 있지 않은 경우가 오히려 많다면서 '이용자의 월별 시뮬레이터 로그인 비율('23년)'이 적게는 %에서 많게는 %라고 제출하였으나, 이는 서비스 Monthly Active Users(MAU, 한 달에 몇 명이나 서비스를 이용하는지를 확인하는 통계)로 오히려 피심인이 시뮬레이터를 통한 개인정보 처리를 적극적으로 통계화하고 있음을 알려주는 것임

개인정보가 유출된 피심인의 스크린골프 서비스 이용자 역시 시뮬레이터와 스크린골프 서비스를 별개의 것으로 인식한다고 볼 수 없고, 피심인이 제출한 개인정보 처리 흐름상으로도 시뮬레이터와 회원 DB간 개인정보 처리 흐름이 연계되어 있는 것으로 확인되며, 피심인의 개인정보 처리방침에도 적용되는 제반 서비스에 시뮬레이터가 명시되어 있는바, 시뮬레이터 판매를 통해 발생한 매출액을 개인정보 처리와 관련 없는 재화 또는 서비스의 매출액으로 인정하거나, 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화 또는 서비스의 매출액이 아닌 것으로 인정하기 어렵다.

특히, 피심인의 시뮬레이터는 일반 기기 판매와 달리, 사업 모델상 이용자의 규모가 가맹점 등 사업자 대상 기기 판매 규모에 절대적 영향력을 행사하는 경우로, 피심인의 사업보고서상에서도 '최종 고객인 골프시뮬레이터 이용자 확보의 중요성'을 언급하면서 "골프시뮬레이터는 최종 이용자의 브랜드 선호도에 따라 스크린골프장의 이용률 및 매출액에 크게 영향을 줄 수 있어 선두 업체는 이용자 확보를 위해… 시뮬레이터와 연동될 수 있는 온라인 포털을 오픈하여 다양한 콘텐츠를 제공한다"는 내용이 명시되어 있다.

< 골프존 사업보고서(2023.3.23.), p34 >

③ 최종고객인 골프시뮬레이터 이용자 확보의 중요성
골프시뮬레이터는 최종 이용자의 브랜드 선호도에 따라 스크린골프방의 이용률 및 매출액에 크게 영향을 줄 수 있습니다. 그렇기 때문에 선두업체는 스크린골프 이용자를 확보하기 위해 시스템적으로 이용자별 난이도를 조정하여 실력에 상관없이 누구나 쉽게 골프를 즐길 수 있게 기능을 부여하고 있으며, 골프시뮬레이터와 연동될 수 있는 온라인 포털을 오픈하여 다양한 컨텐츠를 제공하고 있습니다. 온라인 포털의 경우 이용자에게 코스별 라운드 기록 관리, 코스 이용결과에 대한 상세 분석을 제공하고 있으며, 골프시뮬레이터가 촬영한 이용자의 스윙자세를 온라인 포털내 레슨프로에게 전달하여 스윙자세의 문제점을 체크할 수 있게 구성하고 있습니다. 그리고 전국 시스템을 네트워크로 연결한 골프대회를 개최하여 다양한 이벤트 참여가 가능할 수 있게 구성하고 있으며, 이런 요소들이 종합적으로 결합됨으로써 골프시뮬레이터 브랜드에 대한 로열티(Loyalty)가 강하게 형성되고 있습니다.

기타 판매 매출의 스크린골프장 관리 소프트웨어 제공 매출 중 통화관리매니저 관련 매출 또한 예약관리 및 예약확인 통보(카카오톡)가 가능한 소프트웨어로 스크린골프 서비스 이용자의 개인정보 처리와 관련이 없다고 볼 수 없고, '비즈몰'은 피심인이 스크린골프장 운영 사업주 대상 자재 등 판매를 위해 운영하는 폐쇄형

쇼핑몰이긴 하나, 비즈몰 이용 관련 VOC 처리 과정에서 수집된 사업주들의 이름, 휴대전화번호 등 개인정보가 다량 유출[35]되었으므로 위반행위와 관련 없는 매출로 인정하기 어렵다.

광고 매출은 피심인이 스크린 골프 서비스의 로딩화면이나 피심인의 홈페이지 등에 광고를 노출하고 그에 따른 대금을 받음으로써 발생하는 매출로, 이는 피심인이 다수의 회원을 유치함으로써 광고를 노출하면서 발생한 매출이므로 위반행위와 관련 없는 매출액으로 인정하기 어렵다.

< 서울행정법원 2018. 7. 5., 선고 2017구합53156 판결 >

위반행위와 관련 한 매출액은 개인정보의 유출과 관련하여 직접적으로 영향을 받는 서비스의 매출액 뿐 만 아니라 **간접적으로 영향을 받는 서비스의 매출액도 포함**되는 점, 원고의 **광고 매출은 다수의 회원을 유치하여 원고가 인터넷 쇼핑몰인 인터파크(http://www.interpark.com)를 운영하면서 발생한 것**으로 **회원의 개인정보와 간접적으로는 관련**이 있어 보이는 점, 원고의 카드사 할인 매출 등도 원고의 인터넷쇼핑몰을 이용하는 회원에 의하여 발생한 매출인 점 등에 비추어 보면, 피고의 위 산정방법이 부당하다고 보이지 않으므로 원고의 위 주장은 이유 없다.

그러나, 그 외에 시뮬레이터 판매 중 해외 사업자들에게 수출하여 발생한 매출, 자재 매출 및 기타매출 중 통화관리매니저 관련 매출을 제외한 나머지 매출, 스크린 골프대회 제휴 매출 및 기타 계열사 서비스, 주니어 아카데미, 부동산 임대 매출 등은 위반행위와 관련이 있다고 보기 어려워 제외한다.

3. 위반행위 기간에 대하여

가. 피심인 주장

피심인은 개인정보 유출 사고가 2023년 11월 23일 해커의 공격으로 발생하여 위반 기간이 1년을 초과하지 않는다고 주장한다.

35) 해커에게 유출된 " " 파일 중 상담내역에 사업주들의 개인정보 포함

나. 검토의견 : 불수용

보호법 제64조의2제1항제9호는 안전조치의무를 다한 경우, 과징금을 부과하지 않도록 규정하고, 기존 개인정보 유출 사고에 대한 선례[36] 또한 일관되게 안전조치 의무 위반행위의 기간을 위반행위 기간으로 산정한바, 피심인의 주장을 불수용한다.

법률 해석은 문리해석을 원칙으로 하되, 입법 취지와 목적, 개정연혁, 다른 법령과의 관계 등을 고려하는 체계적·논리적 해석을 보충적으로 할 수 있다.[37]

보호법 제64조의2제1항제9호의 문언은 본문에서 개인정보 유출 등이 된 경우를 '결과 요건'으로 하여 과징금을 부과하도록 하고, 제29조에 따른 안전성 확보조치를 다 한 경우 그러하지 아니한다고 규정하여 그 단서의 '행위 요건'으로 면책시키는 구조로 되어 있다.

기본적인 문언 해석상 보호법 위반'행위'의 기간은 '행위'의 기간을 의미하고, '결과'의 기간을 의미한다고 보기는 어렵다.

또한, 개인정보처리자가 평소에 안전조치의무를 다하였음에도 불구하고 유출 사고가 발생하는 것까지 책임을 부담하게 하는 것은 과하여 면책시키는 것으로 다른 해석의 여지가 없다.

그런데, 본문의 유출 기간을 위반 기간으로 해석하면 본문과 단서의 기간이 다르게 해석됨으로써, 법체계의 일관성을 유지하지 못하고, 위반행위를 억지하고자 하는 과징금의 제재적 처분 성격에 반하게 된다.

특히, 보호법 개정 시 과징금 규정은 정보통신서비스 제공자와의 일원화를 위하여 개인정보처리자와 정보통신서비스 제공자의 과징금 규정을 통합한 것이라고 개정 취지를 밝히고 있고, 주민등록번호 유출과 이용자의 개인정보 유출 규정에 대한 구성요건을 동일하게 '유출 & 안전조치 미비'로 보고 있으므로[38], 개인정보 유출에

36) 개인정보보호위원회 심의·의결(제2024-006-163호, ㈜디지털대성, 2024.3.27.)
37) 대법원 2009. 4.23 선고 2006다81035판결

대한 과징금 규정과 관련하여 보호법 개정으로 과징금 부과 시 위반행위의 기간을 종전과 다르게 보는 것으로 변경되었다고 할 수 없다.

따라서 법 개정 취지에 따르면 정보통신서비스제공자에 대한 과징금 규정 요건은 舊「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 그대로 이관된 것으로, 이관되기 전, 후 법 위반을 다르게 해석할만한 사정 변경이 없으므로 동일하게 해석해야 하고, 이는 소관 업무가 위원회로 이전된 후 2023년 법률이 전면 개정된 후에도 과징금 관련 구성요건은 그대로 유지된 것이므로 위반행위 기간을 안전성 확보조치 미이행 기간으로 해석해야 할 것이다.[39]

4. 과징금·과태료 감경사유에 대하여

가. 피심인 주장

피심인은 현장 조사 및 비대면 조사에 성실히 임하였으며, 자료제출 요구에도 적시에 응하는 등 일관되게 행위 사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력하였으므로 감경 사유에 해당한다고 주장한다.

나. 검토의견 : 수용

피심인이 조사 기간에 위원회의 현장 조사와 자료제출 요구에 대체로 성실히 응하고 행위 사실을 인정한바, 조사에 협력한 것이 인정된다.

---

38) 보호법 개정 시 정무위 검토보고서(92면~94면)

39) 2023년 법 개정 과정에서 종전 규정이 개인정보가 유출되기만 하면 유출과 보호조치 위반과의 관련성이 없어도 과징금을 부과할 수 있는 것으로 해석될 수 있다는 의견을 반영하여 종전 보호법 주민등록번호 유출 과징금 규정의 단서 규정 형태로 수정되었다.(최경진 외 12인 공저, 박영사, 개인정보보호법 760면)

Ⅴ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준[40]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항제9호, 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 부과 수준을 적용한다.'라고 규정하고 있으며, '고려사항별 부과 수준의 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

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

내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 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 유출 등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.'라고 규정하고 있다.

먼저 고의·과실과 관련하여 피심인은 영리를 목적으로 스크린골프 서비스 등을 제공하면서 그 이용자 등의 개인정보가 파일서버를 통해 공유되는 상황조차 인지하지 못하는 등 그에 대한 적절한 보호조치를 하지 않아[41] 221만 건 이상의 개인정보가 유출된바, 피심인에게 중대한 과실이 있으나, 안전조치 의무 위반이 코로나 등 특수한 상황이 계기가 되어 발생하게 된 점, 2013년부터 ISMS 인증을 취득하여 유지하고 있고 ISMS-P 인증심사 수검 중 사고가 발생한 점, 파일서버 외 회원 DB를 포함한 기타 시스템에 대한 조치 등 참작할 사유가 있다는 점을 고려하여 고의·과실은 '중'으로 판단한다.

위반행위의 방법과 관련하여 피심인의 안전조치 의무 위반이 개인정보 유출과 상당한 관련성이 있고, 파일서버에 개인정보 존재 자체를 인지하지 못하여 실질적인 안전성 확보조치에 대한 점검, 관리 및 이행 등 노력은 없었으나, 개인정보 보호 책임자 및 조직이 구성되어 의무사항이 아닌 ISMS-P 인증을 받기 위해 수검에 대응하는 등의 개인정보 보호 노력이 있고, 안전조치 의무 위반이 코로나 등 특수한 상황이 계기가 되어 발생하게 된 점을 고려할 때, 단순 업무 편의를 위해 보안을 약화한 조직적 위반 등 내부 관여가 있었다고 보기 어려운바, 부당성이 현저히 크지는 않으나 상당하므로 '중'으로 판단한다.

위반행위자가 처리하는 개인정보의 유형과 관련하여 유출된 개인정보에 주민등록번호 등 고유식별정보가 포함되어 있어 '상'으로 판단한다.

41) 개인정보가 유출된 파일서버에 대한 관리·감독 없음, 파일 암호화 미조치, 서버 간 원격접속, 서버의 인터넷 통신 등 허용

위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향과 관련하여 피심인이 보유한 통합회원 기준 개인정보의 가 넘는 221만 건 이상의 개인정보가 유출되었고, 안전조치 의무 위반행위 기간은 VPN 기능을 활성화한 2020년 8월 24일부터 2023년 11월 24일까지 3년 이상이며, 다크웹에 개인정보가 게시되는 등 공중에 노출되었고, 이에 전화번호, 이메일 등은 피싱에 이용될 수 있으며, 주민등록번호 및 계좌번호 도용 시 정보주체에게 현저한 피해를 입힐 가능성이 높으므로 '상'으로 판단한다.

따라서, 피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 '매우 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 피심인의 스크린골프, GDR 및 플랫폼 사업 등을 운영하면서 발생한 직전 3개 사업년도의 연평균 전체 매출액에서 관련 없는 매출액을 제외한 천원에 시행령 [별표 1의5] 2. 가. 1)에 따른 '매우 중대한 위반행위'의 부과기준율 1만분의 233을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2020년	2021년	2022년	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 피심인 위반행위의 기간이 2년을 초과('20. 8. 24. ~ '23. 11. 24.)하여 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천 원을 가산하고,

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 조사에 적극 협력한 경우에 해당하여 1차 조정을 거친 금액의 100분의 30에 해당하는 천원을 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 천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•직전 3개 사업연도 연평균 매출액(천원) •연평균 매출액에 2.33% 적용 (매우 중대한 위반)	•위반기간 2년 초과* 50% 가중 (천 원) •취득이익 없으므로 30% 감경 (천 원)	•조사협력으로 30% 감경 (천 원)	**천 원****
⇒ 천 원	⇒ 천 원	⇒ 천 원	

* 위반기간 : '20. 8. 24.(VPN 활성화일) ~ '23. 11. 24. (약 3년 3개월)

※ 암호화 미적용된 문서보안 DRM솔루션 교체는 '22.1월임

** 과징금 부과기준 제11조제5항에 따라 1억원 이상인 경우에는 1백만원 단위 미만의 금액을 버림

2. 과태료 부과

피심인의 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조(과태료) 제2항제5호에 해당하고, 제24조의2(주민등록번호 처리제한)제2항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제8호에 해당하나, 제76조(과태료에 관한 규정 적용의 특례)에 따라 과징금을 부과한 행위와 동일하여 과태료를 부과하지 않는다.

피심인의 제21조(개인정보의 파기)제1항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제4호, 시행령 제63조[별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[42](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 법 제21조(개인정보의 파기)제1항 위반에 대해서는 1회 위반에 해당하는 과태료인 만 원을 기준금액으로 적용한다.

42) 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
마. 법 **제21조제1항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (**과태료의 가중**) 과태료 부과기준 제7조는 '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 제21조(개인정보의 파기)제1항 위반행위에 대하여 과태료 부과기준 제7조에 따라 위반기간이 2년을 초과한 경우로 기준금액의 30%를 가중한다.

2) (**과태료의 감경**) 과태료 부과기준 제6조는 '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 50의 범위 이내에서 감경할 수 있다.' 라고 규정하고 있다.

피심인의 보호법 제21조(개인정보의 파기)제1항 위반행위에 대하여 ▲사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우, ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 점 등을 종합적으로 고려하여 과태료 부과기준 제6조에 따라 기준금액의 40%를 감경한다.

다. 최종 과태료

피심인의 보호법 제21조(개인정보의 파기)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 파기의무 위반	만 원	-	만 원	**만 원**
계				**만 원**

3. 시정조치 명령

피심인의 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조(시정조치 등) 제1항에 따라 개인정보의 보호 및 침해 방지를 위하여 다음과 같이 필요한 조치를 하도록 명한다.

가. 피심인은 회사 내 처리되는 개인정보 처리 흐름을 면밀히 분석하여 내부 관리계획을 재정립하고, 공유설정 등을 통해 개인정보가 유출되지 않도록 조치하는 등 제반 안전조치의무를 준수하는 한편, 피심인이 관리하는 개인정보가 안전하게 처리될 수 있도록 개인정보 보호책임자의 위상과 역할을 강화할 것

나. 전 직원을 대상으로 개인정보 보호 교육을 주기적으로 실시할 것

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

4. 처분 결과 공표명령

보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」[43] (이하 '공표 및 공표명령 지침') 제6조제1항제2호(1천 명 이상 정보주체의 고유식별정보를 유출한 행위)·제3호(매우 중대한 위반행위)·제5호(법 제75조제2항 각호 위반행위 3개 이상)·제7호(위반상태 3년 초과)·제8호(피해를 입은 정보주체의 수가 10만 명 이상)에 해당하고, 제8조, 제11조에 따라 처분 등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분 등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 2분의1 크기로 10일 이상 기간 동안(휴업일 포함) 공표하도록 명한다.

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

Ⅵ. 결론

피심인의 보호법 제21조(개인정보의 파기)제1항, 제24조의2(주민등록번호 처리 제한)제2항, 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제64조의2(과징금의 부과)제1항제9호, 시행령 제60조의2(과징금의 산정기준 등), 제75조(과태료)제2항제4호·제5호·제8호, 제76조(과태료에 관한 규정 적용의 특례), 제64조(시정조치 등)제1항, 제66조(결과의 공표)에 따라 과징금, 과태료, 시정조치 명령, 결과의 공표명령을 주문과 같이 의결한다.

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

이의제기 방법 및 기간

피심인은 이 시정명령 및 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.

2024년 5월 8일

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 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　　조 소 영　(서 명)