방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 13 - 085호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의 결 일 2020. 3. 11.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

가. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

나. 개인정보처리시스템에 접근할 수 있는 개인정보취급자의 비밀번호는 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성, 연속적인 숫자나 생일,

전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고, 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하는 사항 등을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용할 것

다. 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 것

라. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것

마. 정보통신망을 통해 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것

바. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시할 것

2. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 애플리케이션에 1주일 이상 게시하여야 한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

3. 피심인은 제1항부터 제2항까지의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

4. 피심인에 대하여 다음과 같이 과태료 및 과징금을 부과한다.

가. 과 징 금 : 459,000,000원

나. 과 태 료 : 10,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

마. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

이 유

Ⅰ. 기초 사실

(이하 '피심인'이라 한다)은 영리를 목적으로 온라인 교육 서비스를 제공하는 홈페이지( )를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 천원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				
관련 매출				
관련없는 매출				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 검·경 등에서 통보한 피심인에 대하여 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 현장조사(2019.1.11., 1.16.~17., 3.20.~3.21.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 교육 서비스를 제공하는 홈페이지( )를 운영하면서, 2019. 1. 11. 현재 아래와 같이 이용자의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
이용자 정보	(필수)아이디, 비밀번호(암호화), 이름, 이동전화번호 (선택)이메일, 집주소		건

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019.1.11. 방송통신위원회 개인정보 관리 실태 현장조사 시 개인정보 유출 파일과 피심인의 회원정보 DB파일 내용을 대조 한 후 개인정보 유출 사실을 인지

- 2019.1.11. 온라인 개인정보보호 포털(i-privacy.kr)에 개인정보 유출 신고
- 2019.2.12 ~ 3.14. 홈페이지 공지 및 이용자에게 개인정보 유출 통지

※ 이용자 통지는 경찰청 및 방통위 합동조사로 인해 일정을 조정함

2) 개인정보 유출 규모

피심인이 운영 중인 온라인 교육 서비스의 이용자 개인정보 2,113,366건이 미상의 해커에 의해 외부로 유출되었다.

구분	유출 항목	건수
일반회원	아이디, 비밀번호(암호화), 이름, 일반전화번호, 이동전화번호, 이메일, 주소	225,878건
휴면회원	상동	1,473,495건
탈퇴회원		413,991건
합 계		2,113,366건*

* 가입한 이용자 개인정보

3) 유출 경로

- 피심인이 운영 중인 논단기, 업로드 서버의 로그를 분석한 결과, 2018년 4월 20일, 4월 21일, 9월 11일, 12월 4일에 미상의 IP(211.38.63. , 110.47.168. , 171.13.14. , 106.120.161.)에서 홈페이지( )의 게시글 작성 프로그램(Smarteditor v2.3.10) 취약점을 이용해 웹쉘(_20180420_202827_0911159.asp)을 업로드한 후 메인 DB서버의 회원정보를 조회하고 유출한 것으로 추정된다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

1) 피심인은 2013년 12월부터 운영 중인 웹방화벽의 로그에 2018. 4. 20.

211.38.63. , 110,47,168. IP로부터 웹쉘 접근 이력이 남아 있었으나, 업로드 서버( )에서는 접근이 허용된 469건의 웹쉘 접근 이력에 대해 추가적인 개인정보 유출 시도 탐지 및 유출 차단을 위한 조치를 취하지 않은 사실이 있다.

2) 피심인은 개인정보취급자를 대상으로 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하여야 하나, 2019. 1. 16. 기준 개인정보취급자 중 관리자 계정(ID) 비밀번호는 2010. 9. 25. 이후 변경하지 않은 사실이 있다.

3) 피심인은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 하나, 2019. 1. 16. 기준 개인정보처리시스템에 대한 개인정보취급자의 최대 접속시간 제한을 설정하지 않은 사실이 있다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보존 관리하여야 하나, 2019. 1. 16.기준 개인정보취급자가 개인정보처리시스템에 접속한 기록을 2019. 1. 10.부터 2019. 1. 16.까지 7일치를 보존·관리한 사실이 있다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

피심인은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화하여야 하나 2019. 1. 16. 기준 관리자페이지( )의 관리자 아이디를 평문으로 전송한 사실이 있다.

라. 프로그램 업데이트 등 보안조치를 소홀히 한 행위

피심인은 홈페이지( )에 설치된 스마트에디터(Smarteditor) 프로그램(v.2.3.10)에 대하여 2016. 7. 19. 보호나라(boho.or.kr)에 보안공지 된 스마트에디터 2.0(SmartEditor 2.0 Basic 2.8.2.1)을 즉시 업데이트 하지 않고 사용하여 홈페이지 취약점을 방지하지 못한 사실이 있다.

마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2019. 4. 24. '개인정보보호 법규 위반사업자 시정조치(안)사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 5. 22. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)', '백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치(제5호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영(제4호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있고, 제3항은 "정보통신서비스 제공자등

은 접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)'등의 조치를 하여야 한다."라고 규정하고 있으며, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치(제3호)'을 하여야 한다."라고 규정하고, 제5항은 "개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 '고시') 고시 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있고, 제8항은 "정보통신서비스 제공자등은 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성(제1호)', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고(제2호)', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경(제3호)' 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다."라고 규정하고 있으며, 제10항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다."라고 규정하고 있다.

고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처

리시스템에 접속한 기록을 월1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

고시 제6조제3항은 "이용자의 개인정보 및 인증정보를 송수신할 때는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나(제1호), 웹서버에 암호화 응용프로그램을 설치하여(제2호) 전송하는 정보를 암호화하여 송수신하는 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."라고 규정하고 있다.

고시 제7조는 "악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며 '악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시(2호)'를 준수하여야 한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있다.

접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치

하는 것만으로는 부족하며 신규 위협 대응 및 정책의 관리를 위하여 지속적인 업데이트 적용 및 운영·관리, 이상 행위 대응 등의 방법을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있고,

고시 제4조제8항에 대해 정보통신서비스 제공자등은 개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 포함하는 비밀번호 작성 규칙을 수립하고 이를 개인정보처리시스템 등에 적용하여야 하며, 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하고, 개인정보처리시스템에 권한 없는 자의 접근을 방지하기 위하여 비밀번호 등을 일정 횟수 이상 잘못 입력할 때에는 개인정보처리시스템에 접근을 제한하는 등의 보호조치를 추가적으로 적용할 수 있다고 해설하고 있다.

고시 제4조제10항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되도록 최대 접속시간 제한 등의 조치를 취하여야 한다고 해설하고 있다.

고시 제5조제1항에 대해 정보통신서비스 제공자등은 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 한다고 해설하고 있으며,

개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 ⅰ)식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), ⅱ)접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점) 〈년-월-일, 시:분:초〉, ⅲ)접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), ⅳ)수행업무(개인정보처리시스템에서 개인정보취급자가 처리

한 내용을 알 수 있는 정보) 〈개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위〉 등을 포함하는 접속기록을 최소 1년 이상 보존·관리하여야 한다고 해설하고 있다.

고시 제6조제3항에 대해 정보통신서비스 제공자등은 이용자의 성명, 연락처 등의 개인정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, SSL(Secure Sockets Layer) 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화하여 전송하는 방식이며, 응용프로그램을 이용한 보안서버는 웹서버에 접속하여 보안 프로그램을 설치하여 이를 통해 개인정보를 암호화 전송하는 방식이라고 해설하고 있다.

고시 제7조제2호에 대해 응용프로그램이나 운영체계(OS) 보안 취약점 등을 악용하는 악성 프로그램 관련 경보가 발령되었거나, 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있을 때에는 즉시 업데이트를 실시하여야 한다고 해설하고 있다.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}를 소홀히 한 행위

(침입차단시스템 및 침입탐지시스템의 설치·운영) 피심인이 개인정보처리시스템에 대한 불법적인 개인정보 유출시도를 탐지하고도 개인정보 유출을 방지하

기 위한 추가적인 조치를 취하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

(비밀번호 작성규칙) 피심인이 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 사항을 포함하는 비밀번호 작성규칙을 수립하여 이를 적용·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제4호, 고시 제4조제8항을 위반한 것이다.

(최대접속시간) 피심인이 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제10항을 위반한 것이다.

나. 개인정보처리시스템의 접속기록 확인·감독{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록 위·변조}**을 소홀히 한 행위**

피심인이 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보존 관리하지 아니한 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

다. 개인정보의 암호화기술 등을 이용한 보안조치{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인이 관리자페이지( )의 관리자 아이디를 평문으로 전송한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제3호, 고시 제6조제3항을 위반한 것이다.

라. 프로그램 업데이트 등 보안조치{정보통신망법 제28조(개인정보의 보호조치) 중 악성프로그램 방지}**를 소홀히 한 행위**

피심인이 홈페이지( )에 설치된 스마트에디터(Smarteditor) 프로그램(v.2.3.10)에 대하여 2016. 7. 19. 보호나라(boho.or.kr)에 보안공지 된 스마트에디터 2.0(SmartEditor 2.0 Basic 2.8.2.1)을 즉시 업데이트하지 않고 사용하여 홈페이지 취약점을 방지하지 못한 행위는 정보통신망법 제28조제1항제5호, 같은 법 시행령 제15조제5항, 고시 제7조제2호를 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치·운영하지 아니한 행위(고시§4⑤)
			§15②4호	개인정보취급자의 비밀번호 작성규칙을 수립·운영하지 않은 행위(고시§4⑧)
			§15②5호	개인정보취급자의 접속시간이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하지 않은 행위(고시§4⑩)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 최소 1년 이상 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 안전한 해쉬함수 등으로 암호화하지 않고 평문으로 저장한 행위(고시§6①)
	악성 프로그램 방지	§28①5호	§15⑤	응용프로그램 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하지 아니한 행위(고시§7②)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다. 1)정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제

한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것 2)개인정보처리시스템에 접근 할 수 있는 개인정보취급자의 비밀번호는 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성, 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고, 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하는 사항 등을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용할 것 3)개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 것 4)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것 5)정보통신망을 통해 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것 6)악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시할 것

나. 피심인은 가항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지와 모바일 애플리케이션에 1주일 이상 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

<표> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①개인정보처리시스템에 대한 침입차단 및 침입탐지시스템 운영을 소홀히 한 행위, ②개인정보취급자의 비밀번호 작성규칙을 수립·운영하지 않은 행위, ③개인정보취급자의 접속시간이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하지 않은 행위, ④개인정보취급자의 개인정보처리시스템 접속기록을 최소 1년 이상 보존하지 아니한 행위, ⑤개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

V. 과징금 부과

피심인은 정보통신망법 제64조의3제1항제6호에 따라 이용자의 개인정보가 분실·유출된 경우로서 개인정보 보호조치(제28조제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할 수 있다.

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정기준과 산정절차) 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회 고시 제2019-12호, 이하 '과징금 부과기준'이라 한다)' 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 상한액은 같은 법 제64조3의제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, ▲정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 중 접근통제 등을 소홀히 한 피심인에게 이용자의 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 있고,

과징금 부과기준 제5조제3항 단서조항은, 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 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 규정하고 있다.

이에 따라, 피심인이 ▲위반행위로 직접적 이득을 취하지 않았다는 점을 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 정보통신부문 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 원으로 한다.

<정보통신망법 시행령 [별표 8] 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 피심인 위반행위의 기간이 1년 이내 '단기 위반행위'에 해당하므로 기준금액을 유지하고,

최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 원을 감경한다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 피심인이 ▲조사에 성실히 협조한 점 등을 종합적으로 고려하

여 필수적 가중·감경을 거친 금액의 100분의 10에 해당하는 원을 감경한다.

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1) (과징금의 산정기준과 산정절차) 및 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 이상에 해당하여 백만원 미만을 절사한 459,000,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	**최종 과징금***
천원	필수적 가중 없음 필수적 감경 (50%, 천원)	추가적 가중 없음 추가적 감경 (10%, 천원)	**459백만원**
	→ 천원	→ 천원	

* '전기통신사업법 금지행위 위반에 대한 과징금 산정 실무요령'에 따라 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

Ⅵ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조 제1항제3호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

이에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 경우에 해당하므로 기준금액의 100분의 50인 500만원을 가중한다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

기준	가중사유	가중비율
위반의 정도	가. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 너목 가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부 관리계획의 수립·시행을 하지 않은 경우 나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우	

	다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우 라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우 마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치를 하지 않은 경우 바. 정보통신망법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하지 않은 경우

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

이에 피심인이 시정조치(안) 사전통지 및 의견제출 기간 내에 위반행위에 대하여 시정 완료한 점을 고려하여 기준금액의 100분의 50인 500만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2·3·4·5호	1,000만원	500만원	500만원	**1,000만원**
계				**1,000만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,000만원의 과태료를 부과한다.

Ⅶ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

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

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

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 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.

이에 주문과 같이 의결한다.

2020년 3월 11일

위 원 장 한 상 혁 (인)

부위원장 김 석 진 (인)

위 원 허 욱 (인)

위 원 표 철 수 (인)

위 원 김 창 룡 (인)