방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 38 - 173호

안 건 명 개인정보 유출신고 사업자의 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020. 6. 24.

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. 개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화하여 부여할 것

나. 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

다. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 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 과징금 및 과태료를 부과한다.

가. 과 징 금 : 954,000,000원

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

1. (이하 '피심인'이라 한다)은 영리를 목적으로 온라인교육학

원 및 교육정보 제공 사이트」 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 : 백만원)

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

2. 방송통신위원회는 온라인 개인정보보호 포털(i-privacy.kr)에 개인정보 유출을 신고한 피심인에 대하여 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사 하였고, 피심인에 대한 현장조사(2019. 6. 13. ~ 6. 14., 7. 26.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 고등 온라인 교육 사이트 를 2000. 9. 10.부터 운영하면서, 2019. 6. 14.기준 이용자 건의 개인정보를 수집하여 보관하고 있음

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
회원정보 (유효회원)	(필수) 아이디, 비밀번호, 이름, 생년월일, 이메일, 성별, 휴대폰번호, 전화번호, 학교 (선택) 주소, 성적정보, 진학정보, 학년, 계열		건
(휴면회원)	상동		건
(탈퇴회원)	아이디		건
총계			**건**

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019.6.8. 11:16 미상의 해커(이하 '이 사건의 해커'라 한다)로부터 협박메일을 최초 수신한 이후, 2019. 6. 10. 14:36까지 총 9차례에 걸쳐 협박성 메일·게시글 수신
- 2019.6.10. 16:32 개인정보보호 포털(i-privacy.kr)에 개인정보 유출 신고(1차)

※ 개인정보 유출여부는 확인되지 않았으나 해커의 협박이 지속되어 우선 유출 신고

- 2019.6.12. 12:08 이 사건의 해커가 재차 협박하며 탈취한 개인정보 내역 20건을 학습상담게시판에 게시함에 따라 유출사실을 인지
- 2019.6.12. 14:57 개인정보보호 포털에 개인정보 유출 신고(2차)
- 2019.6.13 10:30 전체 회원을 대상으로 개인정보 유출 통지 메일 발송 시작

※ 정확한 유출 대상이 파악되지 않아 '19. 6. 10. 기준 전체 회원 중 유효회원 및 휴면회원 4,940,173건을 대상으로 유출 통지 실시

- 2019.6.13 12:00 피심인의 홈페이지에 개인정보 유출에 관한 안내사항 공지

2) 개인정보 유출 규모

4. 피심인의 DB접근제어솔루션(Chakra Max)의 로그를 분석한 결과, 2019. 6. 7. 기준 5,704,303건의 개인정보가 저장된 _db(, 테이블)에 이 사건의 해커가 접속하여 총 57,295,258 Byte를 조회하였으며, 방화벽 기준 2,884,942,041 Byte를 외부로 유출한 사실이 있으며,

5. 이 사건의 해커는 회원 아이디, 이메일 주소, 핸드폰 번호, 전화번호, 성별, 생년월일, 이름, 비밀번호(암호화)가 포함된 개인정보 20건을 학습상담게시판에 공개한 사실이 있다.

※ 이 사건의 해커가 공개한 20건에 포함되어 있는 s 계정의 정보는 전체 회원 테이블( ) 5,812,408 행 중 5,046,753 행에 저장된 데이터임

< 피심인의 개인정보 유출현황 >

구 분	유 출 항 목	건 수
이용자정보	아이디, 비밀번호(암호화), 이름, 이메일 주소, 핸드폰 번호, 전화번호, 성별, 생년월일 등	5,704,303건

3) 유출 경로

6. 피심인이 2018.6.5.부터 운영하는 앱(실시간질문/답변 서비스)의 사용자 프로필 등록 기능(.aspx)에 업로드 취약점이 존재하여, 2019.5.31.~6.11. 동안 웹 쉘 4종 및 프록시 프로그램이 업로드되어 DB서버에 저장된 개인정보가 유출되었다.

※ 웹쉘 4종 및 프록시 프로그램 : asp13203779190816423 3.cer, test.aspx, tunnel.aspx, tunnel.ashx, / rssocks.exe

※ 웹쉘 접속 해외 IP : 51.158. (프랑스, 클라우드), 52.194. (미국, 클라우드)

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

1) 피심인은 회원정보를 관리하는 관리자 페이지 에 대하여 사내 IP, 개인정보취급자 계정(아이디, 비밀번호) 등으로 접속 제한을 하고 있으나, 2019. 6. 14. 현장조사 과정에서 확인 결과 아이디와 비밀번호로 로그인을 하지 않고도 내부망에서 누구나 특정 주소로 직접 접근하여 개인정보를 조회 및 다운로드 가능하도록 구성한 사실이 있다.

2) 피심인은 2018.5.25. 부터 방화벽, IPS, 웹 방화벽 등의 보안 장비를 운영해 왔으나, 2018.6.5.부터 운영을 시작한 앱에서 사용하는 도메인 을 웹 방화벽 탐지 대상에 등록하지 않고 운영하여, SQL 인젝션 공격 및 웹 쉘 업로드를 인지하지 못한 사실이 있다.

ㄱ. 피심인은 2013.4.13.부터 운영 중인 DB접근제어솔루션를 통하여 개인정보가 담긴 데이터베이스를 대상으로 개인정보 1,000건 이상의 과도한 질의가 있는 경우, DB접근제어 솔루션에서 알람이 발생하도록 설정하여 해커의 공격이 있던 2019.6.7. ~6.11. 동안 알람이 발생하였으나, 2019.6.13. 이후 해당 내용을 확인하였다고 소명한 사실이 있다.

3) 피심인은 앱에서 이미지 업로드 기능 을 자체 개발·운영하는 과정에서 이미지 업로드가 가능한 파일의 확장자(.jpg, png 등)를 제한하는 등 업로드 파일에 대해 확인 과정이 누락되었고, 이미지가 업로드된 웹서버의 디렉토리에 실행 권한이 설정되어 업로드된 웹 쉘이 실행되었다.

나. 처분의 사전통지 및 의견 수렴

8. 방송통신위원회는 2019. 11. 13. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 12. 10. 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)'을 하여야 한다."라고 규정하고 있다.

9. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(개인정보처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '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 있다.

10. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다."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(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있으며 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.

11. '고시 해설서'는 고시 제4조제1항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여하여야 하며 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요가 있으며, 개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 한다고 해설하고 있고, 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 있으며, 제4조제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방

지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 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**

1) (접근권한 최소부여) 피심인이 회원정보를 관리하는 관리자 페이지 에 접속 가능한 계정의 접근권한을 사용자별로 차등부여하지 않고, 내부망에서 누구나 특정 주소로 직접 접근하여 개인정보를 조회 및 다운로드 가능하도록 구성한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제1항을 위반한 것이다.

2) (침입차단 및 탐지시스템의 설치·운영) 피심인이 2018.6.5.부터 운영을 시작한 앱에서 사용하는 도메인( )을 웹 방화벽 탐지 대상에 등록하지 않고 운영하여, SQL 인젝션 공격 및 웹 쉘 업로드를 인지하지 못하였고, DB접근제어솔루션에서 2019. 6. 7.~6. 11. 동안 1,000건 이상의 과도한 질의 행위가 발생하여 알람이 발행하였음에도 불구하고 즉각적인 차단 조치 등을 하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

3) (개인정보 유·노출 방지) 피심인이 2018.6.5.부터 운영하는 앱에 대해

업로드 취약점을 통해 웹쉘이 업로드 되었고 그에 따른 보호조치를 취하지 않아 개인정보가 유출되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 아니한 행위(고시§4①)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치·운영하지 아니한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

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)개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여할 것 2)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 3)취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모

바일 기기에 조치를 취할 것

나. 피심인은 가항부터 다항까지의 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 ① 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 않은 행위 ② 개인정보처리시스템에 침입차단 및 침입탐지시스템 설치·운영을 소홀히 한 행위 ③ 홈페이지 등에 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등 조치를 취하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

12. 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

13. 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.

14. 피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정 기준과 산정절차) 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(이하 '과징금 부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

15. 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

16. 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.

17. 이에 따를 때 정보통신망법 제28조제1항 기술적·관리적 보호조치 중 접근통제를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

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

19. 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.

20. 이에 따라 피심인이 위반행위로 직접적인 이득은 취하지 않았다는 점을 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

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

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2016년	2017년	2018년	평 균
관련 매출액				

※ 자료출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

<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

22. 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내 '단기 위반행위'에 해당하므로 기준금액을 유지하고,

23. 최근 3년간 정보통신망법 제64조의3제1항제6호에 해당하는 행위로 과징금 처분(2018. 7. 4.)을 받아 기준금액 원을 유지한다.

라. 추가적 가중 및 감경

24. 과징금 부과기준 제8조는 사업자의 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.

25. 이에 따를 때 피심인이 ▲개인정보 유출사실을 자진 신고한 점, ▲조사에 성실히 협조한 점을 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 원을 감경한다.

2. 과징금의 결정

26. 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 954,000,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	**최종 과징금***
천원	필수적 가중 없음 필수적 감경 없음	추가적 가중 없음 추가적 감경 (20%, 천원)	**95,400만원**
	→ 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

27. 피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표 9] 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

28. 정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 두 번째에 해당하므로 2회 위반 과태료인 2,000만원을 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 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

29. 그러나 피심인은 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

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 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

30. 이에 따라 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 1,000만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①호	2,000만원	없음	1,000만원	**1,000만원**
계				**1,000만원**

다. 최종 과태료

31. 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 10,000,000원의 과태료를 부과한다.

Ⅶ. 고 발

32. 피심인의 위반행위는 정보통신망법 제28조제1항제2호부터 제5호까지의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 유출한 경우이므로 같은 법 제64조의3제1항제6호에 해당하는 행위가 있다고 인정된다.

33. 또한, 피심인은 최근 3년간 방송통신위원회로부터 과징금 부과('18. 7. 4.)를 받고 동일한 유형의 위반행위를 한 경우로서 같은 법 제73조(벌칙) 및 제69조의2(고발) 규정과 「개인정보보호 법규 위반행위의 고발 등에 관한 기준」 제3조제2항제4호 규정에 따라 수사기관에 고발한다.

Ⅷ. 결론

34. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

35. 피심인은 이 시정명령 및 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일

이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

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

37. 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 6월 24일

위 원 장 한 상 혁 (인)

부위원장 표 철 수 (인)

위 원 허 욱 (인)

위 원 김 창 룡 (인)

위 원 안 형 환 (인)