

방 송 통 신 위 원 회

심의 · 의결

안건번호 제2020-28-122호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020년 5월 19일

주 문

1. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.

2. 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. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 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 불법



적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

다. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 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. 이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리즘으로 암호화하여 저장 할 것

3. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

4. 피심인은 제1항부터 제3항까지의 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.

5. 피심인은 제1항부터 제4항까지의 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.



6. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

가. 과 징 금 : 3,100,000원

나. 과 태 료 : 22,000,000원

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 재능공유 플랫폼 제공 홈페이지() 및 모바일 앱()을 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				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

II. 사실조사 결과

1. 조사 대상

- 2 방송통신위원회는 개인정보보호 포털에 유출신고한 사업자에 대하여 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2019.10.2., 2019.10.4., 2019.10.22.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

- 3 피심인은 재능공유 플랫폼 서비스 제공을 위해 홈페이지()를 운영하면서 2019.10.2. 기준 건의 이용자 정보를 수집·보관하고 있다.

< 개인정보 수집·이용 현황 >

구분	항목	수집일	건수
회원 정보	(필수) 이메일, 비밀번호, 이름, 휴대전화번호 (선택) 성별, 출생년도, 업종, 계좌번호 등		건
	(필수) 이메일, 비밀번호, 이름, 휴대전화번호, 계좌번호, 주민등록번호, 수업소개 (선택) 성별, 출생년도, 업종 등		건
(휴면회원)	분리보관하지 않음		
총 계			건

나. 개인정보 유출 관련 사실관계

- 4 (개인정보 유출 경과 및 대응)



일시		피심인의 유출인지 · 대응 내용
2019.9.30.	19:00	해킹 침입 정황 의심(DB 삭제 확인)
2019.10.1.	14:00	해커 침입 사실 확인(DB내 warning 테이블이 생성됨을 확인) 및 법무법인 의뢰
	19:30	한국인터넷진흥원(KISA)에 신고 및 해당 서버의 운영 중단
	23:00	전체 회원 이메일 공지 및 웹/앱 서비스에 사과문 1차 공지 ※ 개인정보가 삭제되어 해킹 사실을 홈페이지에 공지
2019.10.2.		방송통신위원회 개인정보 현장 조사 후 유출 대상 확인 ※ 유출대상은 운영DB에서 백업 받아둔 DB파일로 확인함
2019.10.3.		유출된 개인정보 확인 시스템 구축 및 2차 공지 ※ 실제 강좌를 개설한 를 대상으로 문자(4,177명) 발송

5 (유출 규모 및 항목) DB 백업파일에 포함된 이용자의 개인정보 380,057건

구분	개인정보 항목
회원정보	이름, 이메일, 비밀번호 혹은 Facebook 계정정보(이메일 또는 전화, 비밀번호)
	[필수] 이름, 태어난 연도, 성별, 소개, 직업, 프로필 사진, 이메일 [선택] 핸드폰번호, 학교, 학과
	[필수] 이름, 태어난 연도, 성별, 소개, 직업, 프로필 사진, 이메일 [선택] 핸드폰번호, 학교, 학과, 계좌번호, 주민등록번호 등

6 (유출 경위) 피심인은 AWS의 DB서버를 카페24로 이전하기 위해 2019.9.16. 테스트 DB서버에 운영 DB()를 백업하여 보관하던 중 2019.9.27. 신원미상의 해커가 알 수 없는 방법으로 테스트 DB서버에 보관 중인 개인정보를 외부로 유출 후 DB를 모두 삭제하였다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실관계

가. 주민등록번호를 수집·이용한 행위

7 피심인은 홈페이지를 통한 등록과정에서 신분확인 및 자격 인증을 위



해 신분증 및 자격증(주민등록증, 운전면허증, 여권, 국가기술자격증, 졸업증명서 등) 사본을 수집하고, 증빙서류 확인 업무가 완료될 경우 수동으로 관련 자료를 삭제하였으나 2019.9.23. 이후 주민등록번호가 포함된 문서(이미지, PDF) 317건을 수집·보유한 사실이 있다.

<주민등록번호가 포함된 신분증 사본 317건>

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

- 8 (안전한 인증수단) 피심인은 2015.12.16.부터 2019.10.2.까지 관리자 페이지 ()를 외부 인터넷망에서 접속할 수 있도록 허용하고 있으나, 안전한 인증 수단을 적용하지 않고 아이디와 비밀번호만으로 접속이 가능하도록 운영하였고, 테스트 DB서버 또한 외부 인터넷망에서 접속을 허용하고 있으나 사내IP 등 제한적 접속 설정 또는 VPN, 전용선 등 안전한 접속수단을 적용하지 않은 사실이 있다.

<관리자 페이지 접속 시 안전한 인증수단 미적용 화면>



- 9 (침입탐지 및 침입차단 시스템 설치·운영) 피심인은 2015.12.16.부터 2019.10.2.까지 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템(웹서버 및 테스트 DB서버)에 접근통제 및 개인정보 유출 시도를 탐지하기 위한 시스템을 설치·운영하지 않은 사실이 있다.

<방화벽 미사용 설정 화면>

- 10 (개인정보 유출 방지조치) 피심인은 인터넷 홈페이지를 통해 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 인터넷 홈페이지에 대한 취약점 점검 수행과 그에 따른 보완 조치 내역 및 테스트 DB서버에 대한 포트(21, 22, 3306) 공유에 대한 취약점 점검 수행과 보완 조치 내역을 증빙할 수 있는 자료를 제출하지 않은 사실이 있다.

다. 개인정보처리시스템에 접속한 기록을 보관하지 아니한 행위

- 11 피심인은 2019.9.16.부터 2019.10.2. 기간 동안 개인정보가 저장된 테스트 DB 서버를 외부에서 접속이 가능하도록 운영한 사실이 있으나, 테스트 DB서버에서 개인정보취급자의 접속 기록·데이터 관리(입력, 수정, 삭제 등) 기록을 확인하기 위한 접속기록을 남기지 않은 사실이 있다.



※ 피심인은 별도의 DB접근제어 솔루션을 운영한 사실이 없으며, Mysql DB의 General Log가 기록되도록 옵션을 활성화하지 않음

라. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

- 12 피심인은 소득신고를 위해 계좌번호 및 주민등록번호를 수집하고 있으나 이용자의 계좌번호 4,944건, 주민등록번호 1,825건 등 총 6,769건을 안전한 암호화 알고리즘을 이용하여 저장하지 않고 평문으로 저장한 사실이 있다.

<평문으로 저장된 주민등록번호 및 계좌번호>



마. 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위

13 피심인은 2019.9.27.기준 1년 이상(마지막 접속이력이 2018.9.26. 이전) 서비스를 이용하지 않은 이용자의 개인정보 85,527건을 파기하거나 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

바. 처분의 사전통지 및 의견 수렴

14 방송통신위원회는 2020. 2. 25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2020. 3. 17. 의견을 제출하였다.

III. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제23조의2제1항은 “정보통신서비스 제공자는 ‘본인확인기관으로 지정받은 경우(제1호)’, ‘법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우(제2호)’, ‘영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우(제3호)’를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.”라고 규정하고 있다.

15 정보통신망법 제23조의2제1항제3호에 따라 고시한 「영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자 고시」 제1조는 “「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2제1항제3호에서 “영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피

한 정보통신서비스 제공자"라 함은 전기통신사업법 제38조 제1항 또는 제2항에 따라 기간통신사업자로부터 이동통신서비스를 도매 제공 받아 재판매하는 전기통신사업자를 말한다. 다만, 본문의 영업상 목적이란 이동전화번호를 이용한 본인확인 서비스를 말한다."라고 규정하고 있다.

- 16 '정보통신서비스 제공자를 위한 개인정보보호 법령 해설서'는 "정보통신망법 제23조의2제1항에 대해 본인확인기관이거나 법령이나 고시에서 주민등록번호의 수집·이용을 허용하는 경우가 아니면 주민등록번호를 수집·이용할 수 없으며, 기존에 보유하고 있는 주민등록번호도 법령 시행 후 2년 이내 파기하도록 하고 있어 2014년 8월 이전까지 삭제하여야 한다."고 해설하고 있다.

나. 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)'를 하여야 한다."라고 규정하고 있다.

- 17 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등을 하여야 한다."라고 규정하고 있다.

- 18 정보통신망법 시행령 제15조제3항은 "접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)', '개인정보처리시스



템에 대한 접속기록을 별도 저장장치에 백업 보관(제2호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

- 19 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제4항은 "정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있고, 제5항은 "정보통신서비스 제공자 등은 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, 제9항은 "정보통신서비스 제공자 등은 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.

- 20 고시 제5조제1항은 "정보통신서비스 제공자 등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상* 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

* 2020.1.2. 시행된 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호)에서는 접속기록을 최소 1년 이상 보존·관리하도록 개정됨

- 21 고시 제6조제2항은 "정보통신서비스 제공자 등은 '주민등록번호(제1호)', '계좌번호(제6호)' 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다."라고 규정하고 있다.



- 22 '고시 해설서'는 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있고,
- 23 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), 웹 방화벽, 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.
- 24 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 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 있다.
- 25 고시 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 방지 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.



26 고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다고 해설하고 있으며,

27 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 처리한 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 6개월 이상 보존·관리하여야 한다고 해설하고 있다.

28 고시 제6조제2항에 대해 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘(보안강도 112비트 이상)으로 암호화하여 저장하여야 하며 처리속도 등 기술발전에 따라 사용 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용 시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인이 필요하다고 해설하고 있다.

다. 정보통신망법 제29조제2항은 “정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.”라고 규정하고 있다.

29 정보통신망법 시행령 제16조제2항은 “이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기



간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.”라고 규정하고 있다.

라. 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. 주민등록번호를 수집·이용{정보통신망법 제23조의2(주민등록번호의 사용 제한)}한 행위

30 피심인은 본인확인기관으로 지정받은 바 없고, 법령 및 고시에서 주민등록번호의 수집·이용을 허용하는 경우에도 해당하지 않으므로 이용자의 주민등록번호를 수집·보유해서는 아니 되나, 이용자의 주민등록번호 317건을 수집·보유한 행위는 정보통신망법 제23조의2제1항을 위반한 것이다.

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

31 (안전한 인증수단) 피심인이 개인정보취급자가 외부에서 피심인의 개인정보처리시스템()에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

32 (침입차단 및 탐지시스템의 설치·운영) 피심인이 개인정보처리시스템(웹서



버 및 테스트 DB서버)에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 및 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 침입탐지시스템을 설치·운영하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

- 33 (개인정보 유출 방지조치) 피심인이 홈페이지를 통해 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 피심인의 홈페이지에 대한 취약점 점검 수행과 그에 따른 보완 조치를 하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

다. 개인정보처리시스템에 접속한 기록{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 보관}을 보관하지 아니한 행위

- 34 피심인이 2019.9.16.부터 2019.10.2.까지 기간 동안 테스트 DB서버에서 개인정보취급자가 접속한 내용을 기록하여 최소 6개월간 보관하지 아니한 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

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

- 35 피심인이 이용자의 주민등록번호, 계좌번호 등 총 7,086건을 안전한 암호알고리즘(보안강도 112비트 이상)으로 암호화하여 저장하지 않은 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제2호, 고시 제6조제2항을 위반한 것이다.

마. 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·



관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

36 피심인이 정보통신서비스를 1년의 기간 동안 이용하지 아니한 이용자의 개인정보 85,527건을 파기하거나 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	주민 등록 번호	§23의2①	-	법적 근거 없이 이용자의 주민등록번호를 수집·이용한 행위
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증 수단을 적용하지 아니한 행위(고시§4④)
	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)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④2호	이용자의 주민등록번호, 계좌번호 등에 대해 안전한 알고리즘으로 암호화 하지 않고 평문으로 DB에 저장한 행위(고시§6②)
	유효 기간	§29②	§16②	1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위

IV. 시정조치 명령

1. 시정명령

가. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.



나. 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) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것 2) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 허가받지 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 모바일 기기에 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) 이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리즘으로 암호화하여 저장 할 것

다. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

라. 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 ①법적 근거없이 이용자의 주민등록번호를 수집·이용한 행위 ②외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위 ③개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치·운영하지 아니한 행위 ④열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위 ⑤개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 최소 6개월 이상 보존하지 아니한 행위 ⑥이용자의 주민등록번호, 계좌번호 등에 대해 안전한 알고리즘으로 암호화 하지 않고 평문으로 DB에 저장한 행위 ⑦1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

- 37 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

- 38 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.
- 39 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 (방송통신위원회 고시 제2019-12호, 이하 '과징금 부과기준'이라 한다)'에 따라



다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

40 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

41 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.

42 이에 따를 때, 정보통신망법 제28조제1항에 기술적·관리적 보호조치 중 접근통제를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

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



44 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.

45 이에 따라, 피심인의 위반행위의 결과가 개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점을 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

46 피심인의 서비스 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.

< 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

- 47 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내 ‘단기 위반행위’에 해당하므로 기준금액을 유지하고,
- 48 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

- 49 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.
- 50 이에 따를 때, 피심인이 ▲개인정보 유출사실을 자진 신고한 점, ▲조사에 성실히 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 원을 감경한다.

2. 과징금의 결정

- 51 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 이하에 해당하여 십만원 미만을 절사한 3,100,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
1억	필수적 가중 없음 (단기위반) 필수적 감경 (50%, 천원)	추가적 가중 없음 추가적 감경 (20%, 천원)	310만원
	→ 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

52 피심인의 정보통신망법 제23조의2(주민등록번호의 사용 제한)제1항, 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항에 대한 과태료는 같은 법 제76조제1항제2호·제3호·제4호, 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

53 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 각 적용한다.

〈 위반 횟수별 과태료 금액 〉



위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
다. 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	법 제76조 제1항제2호	1,000	2,000	3,000
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
더. 법 제29조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 하지 아니한 자	법 제76조 제1항제4호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보 제공 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.

54 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 3개인 경우에 해당하므로 기준금액의 50%인 500만원을 가중하고 같은 법 제23조의2제1항 및 제29조제2항 위반행위에 대해서는 특별히 가중할 사유가 없으므로 가중하지 않는다.

< 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 자금 사정, ▲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.

55 이에 따라 피심인의 정보통신망법 제23조의2제1항 위반행위에 대해서 소기업으로 평균 당기순이익이 적자인 점을 고려하여 기준금액의 30%인 300만원을 감경하고, 같은 법 제28조제1항 및 제29조제2항 위반행위에 대해서는 시정 조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§23의2①	1,000만원	없음	300만원	700만원
§28①2·3·4호	1,000만원	500만원	500만원	1,000만원
§29②	1,000만원	없음	500만원	500만원
계				2,200만원



다. 최종 과태료

- 56 이에 따라 피심인의 정보통신망법 제23조의2제1항, 제28조제1항 및 제29조 제2항 위반행위에 대해 22,000,000원의 과태료를 부과한다.

VII. 결론

- 57 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제2호·제3호·제4호(과태료)에 따라 주문과 같이 결정한다.

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 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 5월 19일

위원장 한 상 혁



부위원장 표 철 수



위 원 허 욱



위 원 김 창 룡



위 원 안 형 환

