# 방 송 통 신 위 원 회
# 심의 · 의결

**안건번호** 제2019 - 44 - 263호

**안 건 명** 등 50개사 개인정보보호 법규 위반에 대한 시정조치에 관한 건

**피 심 인** **(사업자등록번호 : )**

**대표이사**

**의 결 일** 2019. 9. 6.

## 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. 개인정보보호 조직의 구성 및 운영에 관한 사항과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 정기적인 교육에 관한 사항을 포함하여 개인정보 안전성 확보를 위하여 필요한 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성프로그램 방지, 출력·복사 시 보호조치) 이행을 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행할 것

나. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터

등을 물리적 또는 논리적으로 망분리할 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

라. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

2. 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.

3. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

가. 과 징 금 : 81,200,000원

나. 과 태 료 : 15,000,000원

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)는 영리를 목적으로 식품배송 사이트를 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 >

| 대표자 | 설립일자 | 자본금 | 주요서비스 | 종업원 수 |
|---|---|---|---|---|
| | | | | |

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 백만원)

| 구 분 | 2014년 | 2015년 | 2016년 | 평균 |
|---|---|---|---|---|
| 매출액 | | | | |
| 정보통신서비스 | | | | |

※ 자료 출처 : 피심인이 제출한 자료

## Ⅱ. 사실조사 결과

### 1. 조사 대상

방송통신위원회는 서울동부지방검찰청으로부터 개인정보 유출 사업자에 대한 자료를 전달받아 피심인을 대상으로 정보통신망법 위반여부에 대한 개인정보 취급·운영 실태를 현장조사(2018. 1. 15.~2018. 1. 16.)하였고, 다음과 같은 사실을 확인하였다.

### 2. 행위 사실

### 가. 개인정보 수집현황

피심인은 식품 배송 사이트 를 운영하면서 2018. 1. 15. 기준으로 건의 회원정보를 수집·보관하고 있다.

< 피심인의 개인정보 수집 현황 >

| 구 분 | 항 목 | 수집일 | 건수 |
|---|---|---|---|
| 이용자 정보 (유효회원) | (필수) 아이디, 비밀번호, 이름, 이메일, 휴대전화번호<br>(선택) 생년월일, 성별 | | |
| 휴면회원 | 상동 | | |

## 나. 개인정보 유출 규모 및 경로

### (1) 개인정보 유출 규모

피심인이 식품 배송 사이트를 운영하면서 수집한 회원의 개인정보 101,866건이 유출되었다.

< 피심인의 개인정보 유출 현황 >

| 구분 | 유 출 항 목 | 건 수 |
|---|---|---|
| 회원 | 아이디, 비밀번호, 이메일, 일반전화번호, 휴대전화전호 | 101,866건 |

### (2) 유출 경로

미상의 해커가 2017. 9. 15.~16., 9. 20. 3일간 SqlMap 툴을 사용하여 SQL Injection 방법으로 피심인의 쇼핑몰 사이트를 공격하여 피심인의 이용자 개인정보가 유출되었다.

### (3) 유출 인지 및 대응

피심인은 2017. 9. 20. 사용 중인 서버에서 오류가 발생했다는 메시지를 확인

하고 해당 로그를 확인한 결과, SQL Injection 공격으로 피심인의 이용자 개인정보가 유출된 것을 파악하고 해커로 의심되는 아이피(IP)를 차단한 후 같은 날 한국인터넷진흥원(krcert.or.kr)에 해킹사고 신고를 하였으며, 2017. 9. 21. 개인정보보호 포털(i-privacy.kr)에 유출신고를 하고, 전체 이용자에게 개인정보 유출 사실을 이메일로 통지하였다.

**3. 개인정보의 기술적·관리적 보호조치 등 사실 관계**

**가. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행**{정보통신망법 제28조(개인정보의 보호조치) 중 내부관리계획}**을 하지 않은 행위**

피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 사항 등을 규정한 계획, 지침 등을 수립하지 않은 사실이 있다.

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

**1) (망분리)** 피심인은 2016년도 매출액이 약 170억원인 정보통신서비스 제공자임에도 불구하고, 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적·논리적으로 망분리한 사실이 없다.

**2) (취약점 점검)** 피심인은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치(인터넷 홈페이지의 취약점 점검 등)를 취한 사실이 없다.

**다. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}을 소홀히 한 행위**

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않았으며, 데이터베이스(DB) 및 관리자페이지의 접속기록을 보관하지 않은 사실이 있다.

**라. 처분의 사전통지 및 의견 수렴**

방송통신위원회는 2018. 9. 18. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 10. 16. 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 '개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행(제1호)', '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)', '접속기록의 위조·변조 방지를 위한 조치(제3호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제1항은 "정보통신서비스 제공자등은 개인정보의 안전한 처리를 위하여 '개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항(제1호)', '정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자의 교육에 관한 사항(제2호)', '개인정보 보호조치를

이행하기 위하여 필요한 세부 사항(제3호)'의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다."라고 규정하고 있고, 제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자의 경우 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'를 하여야 한다."라고 규정하고 있으며, 제3항은 "정보통신서비스 제공자등은 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 있고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적 기준을 정하여 고시하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시'라 한다라 한다) 제3조제3항은 "개인정보보호 조직의 구성·운영과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 교육의 세부계획, 고시 제4조부터 제8조까지의 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성 프로그램의 방지, 물리적 접근 방지) 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다."라고 규정하고 있다.

제4조제6항은 "전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하여야 한다."고 규정하고 있고, 제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에

게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

제5조제1항은 "개인정보취급자가 개인정보 처리시스템에 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.

'고시 해설서'는 고시 제3조제3항에 대해 정보통신서비스 제공자등은 스스로의 환경을 고려하여 내부관리계획의 수립에 관한 사항을 마련하여야 하며, 내부관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 사업자 또는 대표자에게 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알리고 이를 준수할 수 있도록 하여야 한다고 해설하고 있다.

고시 제4조제6항에 대해 정보통신서비스 제공자등이 망분리를 할 때 인터넷망으로부터 분리되어야 하는 대상은 개인정보처리시스템에서 개인정보를 다운로드(개인정보처리시스템에 직접 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일형태로 저장하는 것), 파기(개인정보처리시스템에 저장된 개인정보 파일, 레코드, 테이블 또는 데이터베이스를 삭제하는 것) 및 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등이며 스스로의 환경에 맞는 망분리를 적용하여 개인정보를 처리하는 과정에서 외부와의 접점을 최소화함으로써 외부로부터 들어오는 공격이나 내부에서 외부로의 개인정보 유출 등을 차단하여야 한다고 해설하고 있고, 제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 인터넷 홈페이지 운영 관리 시 1)보안대책을 정기적으로 검토, 2)홈페이지 게시글, 첨부파일 등에 개인정보 포함 금지, 정기적 점검 및 삭제 등의 조치, 3) 서비스 중단 또는 관리되지 않는 홈페이지는 전체삭제 또는 차단조치, 4) 공격패턴, 위험분석, 침투 테스트, 등을 수행하고 발견되는 결함에 따른 개선 조치, 5) 취약점을 점검(취약점 점검 시에는 기록을 남겨 추적성 확보 및 향후 개선조치 등에

활용할 수 있도록 할 필요가 있으며 정기적으로 웹셸 등을 점검하고 조치한다면 취급중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다)하고 그 결과에 따른 적절한 개선조치 등 개인정보 유·노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선조치를 하여야 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 하며, 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 아이디 등), 접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점) 〈년-월-일, 시:분:초〉, 접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), 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.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 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. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행**{정보통신망법 제28조(개인정보의 보호조치) 중 내부관리계획}**을 하지 않은 행위**

피심인이 개인정보보호 조직의 구성·운영과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 교육의 세부계획, 고시 제4조부터 제8조까지의 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성 프로그램의 방지, 물리적 접근 방지) 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하지 않은 행위는 정보통신망법 제28조제1항제1호, 같은 법 시행령 제15조제1항, 고시 제3조제3항을 위반한 것이다.

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

**1) (망분리)** 피심인이 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리를 하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제3호, 고시 제4조제6항을 위반한 것이다.

**2) (취약점 점검)** 피심인이 인터넷 홈페이지의 취약점 점검 등을 통해 개인정보가 유·노출되지 않도록 조치하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

**다. 개인정보처리시스템에 접속한 기록의 보관 및 점검**{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인이 개인정보취급자의 개인정보처리시스템 접속일시, 처리내역 등 접속기록을 작성하여 월 1회 이상 이를 확인·감독하지 않고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15

조제3항제1호, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

| 사업자 명 | 위반 내용 | 법령 근거 | | |
|---|---|---|---|---|
| | | 법률 | 시행령 | 세부내용(고시 등) |
| | 내부 관리 계획 | §28①1호 | §15① | 개인정보의 안전성 확보를 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행하지 않은 행위(고시§3③) |
| | 접근 통제 | §28①2호 | §15②3호 | 개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리하지 않은 행위(고시§4⑥) |
| | 접근 통제 | §28①2호 | §15②5호 | 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨) |
| | 접속 기록 | §28①3호 | §15③1호 | 개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월 1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 않은 행위(고시§5①) |

## Ⅳ. 시정조치 명령

### 1. 시정명령

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) 개인정보보호 조직의 구성 및 운영에 관한 사항과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 정기적인 교육에 관한 사항을 포함하여 개인정보 안전성 확보를 위하여 필요한 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성프로그램 방지, 출력·복사 시 보호조치) 이행을 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행할 것 2) 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리할 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 6개월 이상 접속기록을 보존·관리할 것

### 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

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 〔별표 8〕(과징금의 산정기준과 산정절차) 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회 고시 제2015-30호, 이하 '과징금 부과기준'이라 한다)' 따라 다음과 같이 부과한다.

### 1. 과징금 상한액과 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 상한액은 같은 법 제64조 3의제1항, 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 따라, ▲정보통신망법 제28조제1항제2호에 따른 접근통제 중 기술적·관리적 보호조치 중 개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리하지 않은 행위, ▲정보통신망법 제28조제1항제2호에 따른 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위, ▲정보통신망법 제28조제1항제3호에 따른 개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월 1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 않은 행위 등 보호조치를 소홀히 한 피심인에게 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, 피심인의 위반행위의 결과가 ▲개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점, ▲유출된 개인정보가 피심인이 보유하고 있는 개인정보의 100분의 5 이상(2018. 1. 15. 기준, 피심인의 서비스인 이용자의 개인정

보 건 중 101,866건 유출)인 점, ▲이용자의 개인정보가 공중에 유출된 점 등을 종합적으로 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 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.[1)]

< 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 위반행위의 기간이 1년 이내('17.9.15.~'17.9.21.)이므로 기준금액을 유지하고,

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

**라. 추가적 가중 및 감경**

1) 제2019-41차 회의('19.8.23.) 시 착오에 의해 위반행위와 관련한 매출액을 '15년~'17년의 연평균 매출액으로 산정하였으나, 제2019-44차 회의('19.9.6.)에서 피심인의 위반행위 직전 3개 사업연도인 '14년~'16년의 연평균 매출액으로 산정하는 것으로 수정 의결함

특별히 추가적으로 가중할 사항은 없으며, 방송통신위원회의 조사에 적극 협력한 점을 고려하여 100분의 20인 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 미만에 해당하여 십만원 미만을 절사한 81,200,000원을 최종 과징금으로 결정한다.

< 과징금 산출내역 >

| 기준금액 | 필수적 가중감경 | 추가적 가중감경 | **최종 과징금*** |
|---|---|---|---|
| 원 | 필수적 가중 없음<br>필수적 감경<br>(50%, 원) | 추가적 가중 없음<br>추가적 감경<br>(20%, 원) | **81,200천원** |
| | → 원 | → 원 | |

* '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 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.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위가 3개에 해당하므로 기준 금액의 50%인 500만원을 가중한다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

| | | |
|---|---|---|
| 위반의 정도 | 가. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우 | 기준금액의 50% 이내 |
| | **제3호 정보통신망법 시행령 제74조별표 9 제2호 너목** | |

| | |
|---|---|
| | 가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행을 하지 않은 경우<br>나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우<br>다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우<br>라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우<br>마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치를 하지 않은 경우<br>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.

그러나 피심인의 정보통신망법 제28조제1항 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

| 위반조문 | 기준금액 | 가중 | 감경 | 최종 과태료 |
|---|---|---|---|---|
| §28①1·2·3호 | 1,000만원 | 500만원 | 없음 | **1,500만원** |
| 계 | | | | **1,500만원** |

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,500만원의 과태료를 부과한다.

< 위반행위별 과징금 · 과태료와 시정명령 >

| 위반 유형 | 과징금 | 과태료 | 시정명령 | 계 |
|---|---|---|---|---|
| 기술적·관리적 보호조치 §28①1·2·3호 | 8,120만원 | 1,500만원 | | 9,620만원 |

## 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.

2019년 9월 6일

위 원 장 이 효 성 (인)

부위원장 김 석 진 (인)

위 원 허 욱 (인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)