# 방 송 통 신 위 원 회
# 심의·의결

**안건번호** 제2017 - 04 - 024호

**안 건 명** 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

**피 심 인** (사업자등록번호 :

**대표**

**의 결 일** 2017. 1. 26.

## 주 문

1. 피심인은 본인확인기관으로 지정받은 바 없고, 법령, 고시에서 주민등록번호 수집·이용을 허용하는 경우에도 해당하지 아니하므로 이용자의 주민등록번호를 보유하여서는 안 되고, 피심인이 개인정보처리시스템에 보유하고 있던 이용자의 주민등록번호 2,959건을 모두 파기하여야 한다.

2. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보의 도난·유출을 방지하기 위하여 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 기술적·관리적 보호조치를 하여야 한다.

3. 피심인은 제1항 및 제2항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 도난·유출을 방지하기 위한 재발 방지대책을 수립하여 2017. 3. 31.까지 방송통신위원회에 보고하여야 한다.

4. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 25,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

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

## 이 유

### Ⅰ. 기초 사실

피심인은 영리를 목적으로 인터넷설치·판매 등 영업을 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항 제3호에 따른 정보통신서비스 제공자이고, 피심인이 제출한 자료에 따르면 '15년 매출액은 약 원, '15년 상시 종업원 수는 이다.

### Ⅱ. 사실조사 결과

#### 1. 조사대상

부산지방경찰청이 인터넷에 개인정보 DB를 판매한다고 광고를 게재한 개인정보 판매상을 추적하던 중, 개인정보 침해위협이 높은 피심인의 사이트를 인지하여 방송통신위원회에 통보(2016.5.19.)해 옴에 따라, 방송통신위원회는 정보통신

망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사(2016.9.7.~2016.9.8.)하였고, 다음과 같은 사실을 확인하였다.

## 2. 행위사실

가. 주민등록번호를 파기하지 않은 행위(정보통신망법 부칙 제2조, 제23조의2 제1항)

피심인은 정보통신망법에 의해 주민등록번호 수집·이용을 허용 받은 사업자에 해당하지 아니하여, 2012. 8. 18.부터는 주민등록번호를 수집·이용할 수 없고, 2014. 8. 17.까지는 보유하고 있는 주민등록번호를 파기하여야 함에도, 피심인은 이용자의 주민등록번호 2,959건을 보유하였다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위(정보통신망법 제28조제1항)

피심인은 개인정보취급자가 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속이 가능하도록 하여 안전한 인증수단을 적용하지 않았고, 이용자의 개인정보에 해당하는 주민등록번호 2,959건, 신용카드번호 63건, 계좌번호 21,075건을 개인정보처리시스템에 암호화하지 않고 저장하였으며, 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않았다.

다. 사전통지 및 의견수렴

방송통신위원회는 2016. 12. 1. '개인정보보호 법규 위반사업자 사전통지 및 의견수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2016. 12. 26. 의견을 제출하였다.

## Ⅲ. 위법성 판단

### 1. 관련법 규정

가. 정보통신망법 제23조의2제1항은 "정보통신서비스 제공자는 '제23조의3에 따라 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."고 규정하고 있다.

나. 정보통신망법 부칙(법률 제11322호, 2012.2.17.) 제1조는 "이 법은 공포 후 6개월이 경과한 날부터 시행한다."라고 규정하고 있고, 제2조제1항은 "이 법 시행 당시 주민등록번호를 사용한 회원가입 방법을 제공하고 있는 정보통신서비스 제공자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제23조의2제1항 각 호의 어느 하나에 해당하는 경우는 제외한다."라고 규정하고 있으며, 제2조제2항은 "제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제23조의2제1항의 개정규정을 위반한 것으로 본다."라고 각 규정하고 있다.

다. 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 접근통제장치의 설치·운영(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등(제4호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시

스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)' 등의 조치를 하여야 한다."고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)' 및 '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치(제3호)' 등의 보안조치를 하여야 한다."고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준」(이하 '고시'라 한다) 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."고 규정하고 있고, 제6조제2항은 "정보통신서비스 제공자등은 주민등록번호, 신용카드번호, 계좌번호 등에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다."라고 규정하고 있으며, 제6조제3항은 "정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능이나 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능 중 하나의 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준 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 인증 수단의 적용이 필요하다고 해설하고 있다.

라. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등

이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다."라고 규정하고 있다.

## 2. 위법성 판단

가. 주민등록번호를 파기하지 않은 행위(정보통신망법 부칙 제2조, 제23조의2 제1항)

피심인은 본인확인기관으로 지정받은 바 없고 법령, 고시에서 주민등록번호 수집·이용을 허용하는 경우에도 해당하지 아니하여 이용자의 주민등록번호를 수집·이용할 수 없음에도, 이용자의 주민등록번호 2,959건을 보유하여, 위 부칙 제2조제2항에 따라 정보통신망법 제23조의2제1항을 위반하였다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위(정보통신망법 제28조제1항)

피심인은 개인정보취급자가 외부에서 피심인의 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하여 추가적으로 안전한 인증수단을 적용하지 않았고, 이용자의 주민등록번호 2,959건, 신용카드번호 63건, 계좌번호 21,075건을 개인정보처리시스템에 암호화하지 않고 저장하였으며, 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제)·제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제2항·제4항, 고시 제4조제4항 및 제6조제2항·제3항을 위반하였다.

< 보호조치 의무 관련 피심인의 위반사항 >

| 사업자명 | 위반 내용 | 법령 근거 | | 세부내용(고시 등) |
|---|---|---|---|---|
| | | 법률 | 시행령 | |
| (주 ·) | 접근 통제 | §28① 2호 | §15② 1호 | 외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④) |
| | 암호화 | §28① 4호 | §15④ 2호 | 이용자의 신용카드번호 63건, 계좌번호 21,075건을 개인정보처리시스템에 암호화하지 아니하고 저장한 행위(고시§6②) |
| | 암호화 | §28① 4호 | §15④ 3호 | 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않은 행위(고시§6③항) |

## Ⅳ. 시정조치 명령

### 1. 시정명령

가. 피심인은 본인확인기관으로 지정받은 바 없고, 법령, 고시에서 주민등록번호 수집·이용을 허용하는 경우에도 해당하지 아니하므로 이용자의 주민등록번호를 보유하여서는 안 되고, 피심인이 개인정보처리시스템에 보유하고 있던 이용자의 주민등록번호 2,959건을 모두 파기하여야 한다.

나. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보의 도난·유출을 방지하기 위하여 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 기술적·관리적 보호조치를 하여야 한다.

## 2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 도난·유출을 방지하기 위한 재발방지대책을 수립하여 2017. 3. 31.까지 방송통신위원회에 보고하여야 한다.

## 3. 과태료 부과

피심인의 정보통신망법 제23조의2(주민등록번호의 사용제한)제1항 및 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제2호·제3호, 같은 법 시행령 제74조의 [별표 9] 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '처리지침')에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 '처리지침' 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하여 각각 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

| 위반사항 | 근거법령 | 위반 횟수별 과태료 금액(만원) | | |
|---|---|---|---|---|
| | | 1회 | 2회 | 3회 이상 |
| ○ 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우 | 법 제76조 제1항제2호 | 1,000 | 2,000 | 3,000 |
| ○ 법 제28조제1항(법 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)** '처리지침' 제9조는 ▲위반행위가 2개 이상인 경우, ▲위반행위가 2개 이상에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기·정도, 사회·경제적 파급 효과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 정보통신망법 제28조제1항 위반 행위에 대해서는 위반행위가 2개로 위반행위의 정도가 심하다고 판단되므로, 기준금액의 2분의 1인 500만원을 가중한다.

다만, 정보통신망법 제23조의2제1항을 위반하여 주민등록번호를 파기하지 않은 행위에 대해서는 과태료를 가중할 필요가 있는 경우에 해당하지 않는 바, 피심인에 대한 과태료를 가중하지 않는다.

2) **(과태료의 감경)** '처리지침' 제8조는 ▲위반행위의 결과가 과실에 의한 경우, ▲위반행위의 결과가 경미한 경우, ▲위 두 가지 규정에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우에는 '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 경우 각 위반행위가 과실에 의한 것이라 볼 수 없고 사업 규모가 영세하지 않는 등 과태료를 감경할 필요가 있는 경우에 해당하지 않는 바, 피심인에 대한 과태료를 각각 감경하지 않는다.

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제23조의2제1항 및 제28조제1항 위반에 대

해 2,500만원의 과태료를 부과한다.

< 과태료 산출내역 >

| 위반조문 | 기준금액 | 과태료 가중 | 과태료 감경 | 최종 과태료 |
|---|---|---|---|---|
| §23조의2① | 1,000만원 | 없음 | 없음 | **1,000만원** |
| §28①2·4호 | 1,000만원 | 500만원 | 없음 | **1,500만원** |
| 계 | | | | **2,500만원** |

## 4. 과징금 부과

피심인의 경우, 부산지방경찰청이 인터넷에서 개인정보 DB를 판매한다고 광고를 게재한 개인정보 판매상을 추적하던 중 개인정보 침해위협이 높은 사업자로 인지되었으나, 실제 유출 DB 및 로그기록이 남아 있지 않아 개인정보가 유출된 증거와 유출 시점 등을 파악할 수 없었으므로, 과징금은 부과하지 않는다.

## V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제76조제1항제2호·제3호(과태료)에 따라 주문과 같이 결정한다.

## 이의제기 방법 및 기간

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

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조 규정에 의하여 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면

으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항 규정에 의하여 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 과태료를 납부하여야 한다.

위 원 장 최 성 준 (인)

부위원장 김 재 홍 (인)

위 원 김 석 진 (인)

위 원 이 기 주 (인)

위 원 고 삼 석 (인)