방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 04 - 030호

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 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 하는 등 기술적·관리적 보호조치를 하여야 한다.

2. 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.

이 유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 온라인 대부중개 사업을 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인이 제출한 자료에 따르면 최근 1년('15년 하반기~'16년 상반기) 매출액은 약 이며, '16년 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 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사(2016.9.23.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 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 않았다.

나. 사전통지 및 의견제출

방송통신위원회는 2016. 12. 1. '개인정보보호 법규 위반사업자 사전통지 및 의견수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2016. 12. 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 접근통제장치의 설치·운영(제2호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

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

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제4조제4항에 대

해 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.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 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. 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 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제4항을 위반하였다.

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 보관, 관리하는 자로서 개인정보의 도난·유출을 방지하기 위하여 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불

어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하는 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 제28조제1항(개인정보의 보호조치) 위반에 대하여는 3,000만원 이하의 과태료를 부과할 수 있다.

그러나 피심인은 ▲위반행위가 1개에 불과하고 이에 대해 시정조치한 점, ▲ 영세한 소상공인 기업인 점 등을 감안하여 이번에 한해 과태료를 부과하지 않는다.

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)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.

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)