방 송 통 신 위 원 회
심의 · 의결

안건번호 제2018 - 35 - 388호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2018. 7. 11.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한함으로써 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.

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 과태료를 부과한다.

가. 금　　액 : 10,000,000원

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 홈페이지(　　)를 통해 자동차 관련 제품(네비게이션, 필름 등)을 소개·판매하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈참고 1〉 피심인의 일반현황

대표이사	설립일자	자본금	주요서비스	종업원 수

〈참고 2〉 피심인의 최근 3년간 매출액 현황

(단위 백만원)

구　분	2015년	2016년	2017년	평 균
매출액				
정보통신부문 매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

경찰청이 ‘ ’ 해커를 추가 조사하는 과정에서 피심인의 개인정보가 유출되었다는 내용을 방송통신위원회에 알려옴('18.1.24.)에 따라, 방송통신위원회는 피심인을 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2018.3.6.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘ 제품 소개·판매’ 홈페이지( )의 회원가입을 통해 20,732건의 개인정보를 수집하였으나, 2015년 4월 사업지속 여부, 사이트 유지 비용 등의 문제로 로그인 기능을 제거하고, 2016년말 DB 내 회원정보가 저장된 테이블(Table)을 파기하였다.

나. 개인정보 유출 규모 및 경로

(1) 개인정보 유출규모

피심인이 운영하는 제품 판매 및 소개 사이트( ) 이용자 20,732건의 개인정보가 유출되었다.

〈참고 3〉 피심인의 개인정보 유출 현황

구 분	유 출 항 목	건 수
이용자	아이디,이름,이메일,집전화번호,휴대폰번호,주소	20,732건

(2) 유출 경로

숙박앱 '어기어때'를 해킹한 해커가 2016.10.29. 사이트( )의 업로드 취약점 공격을 통해 개인정보를 유출한 것으로 추정된다.

(3) 유출 신고

피심인은 2018.3.08. 서울전파관리소 연락을 받은 후 개인정보 유출을 인지하고, 2018.3.09. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 유출을 신고하였으나, 회원정보 파기로 이용자 연락처 등이 없어 이용자 통보는 하지 않고 홈페이지에 유출사실을 공지하였다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

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

피심인은 침입차단 및 탐지시스템(UTM 장비 : Sophos SG210)을 설치하고 있었으나, 해커에 의해 악성프로그램(웹쉘) 파일이 서버에 업로드('16.10.29.) 되고 개인정보 유출사건에 대해 경찰청의 수사('17.7.5.)가 있기 전까지 개인정보처리시스템에 불법적인 접근 및 유출을 탐지하지 못한 사실이 있다

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 4. 26. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 5. 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)' 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 조치를 하여야 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 한다) 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 있다.

나. 정보통신망법 제64조제3항은 "과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반 한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 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**

고시 제4조제5항의 입법 목적은 '정보통신망을 통한 불법적인 접근 및 침해사고 방지'인 바, 그 내용은 첫째 침입차단 및 침입탐지 기능을 포함한 시스템의 '설치' 의무이고, 둘째 침입차단 및 침입탐지 기능을 포함한 시스템의 '운영' 의무이다.

먼저 시스템 '설치' 의무에 대하여 살펴보면, 정보통신서비스 제공자등은 ①접속권한을 IP주소 등으로 제한하여 비인가 접근을 '차단'하는 기능(침입차단 기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출 시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

피심인이 침입차단 및 침입탐지 시스템을 통해 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출을 탐지하지 못한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제5항을 위반한 것이다.

〈참고 4〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하고 개인정보처리시

스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.

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.

3. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '과태료 부과 등 처리지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

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

〈참고 5〉 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·감경

특별히 과태료를 과중·감경할 사유가 없어 기준금액을 유지한다.

〈참고 6〉 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	1,000만원	없음	없음	**1,000만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,000만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제3호에 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.

위 원 장 이 효 성 (인)

부위원장 허 욱 (인)

위 원 김 석 진 (인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)