방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 35 - 386호

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 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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

다. 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 것

3 피심인은 제1항부터 제2항까지의 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.

4 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 20,000,000원

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　　서비스를 제공하는 「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				

※ 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(2018.2.19.~2018.2.20.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘ ’ 서비스를 운영하면서 2018. 2. 19. 기준으로 400건의 회원정보를 보유하고 있다.

〈참고 3〉 피심인의 개인정보 수집 현황

구 분	항 목	수집기간	건수
사이트 회원	[필수] 아이디, 비밀번호, 이름, 휴대전화번호, 이메일	'01.2.10. ~	400건

나. 개인정보 유출 규모 및 경로

(1) 개인정보 유출규모

피심인의 서비스를 이용하던 사업자(99개)가 보유한 1,937,799명의 개인정보가 유출되었다.

〈참고 4〉 피심인의 개인정보 유출 현황

구 분	유 출 항 목	건 수
99개 솔루션 이용 고객사의 회원정보	아이디, 성명, 생년월일, 이메일, 주소, 전화번호 등	1,937,799건

(2) 유출 경로

숙박앱 ' ' 를 해킹한 해커가 2016.12.18. 크로스사이트 스크립트 공격(XSS공격)[1]을 통해 관리자페이지 로그인 세션값을 탈취 후 고객사별 관리자페이지에서 접속하여 회원정보를 엑셀로 다운로드하여 개인정보를 유출한 것으로 추정된다.

(3) 유출 신고

피심인은 경찰청이 2017.7.13. 숙박앱 ' ' 를 해킹한 해커 일당에게

1) XSS(Cross Site Scripting) 공격 : 게시물에 실행코드와 태그의 업로드가 규제되지 않는 경우 이를 악용하여 열람한 타 사용자의 PC로 부터 정보를 유출하는 해킹 기법으로 사용자의 세션값을 탈취하거나, 웹 사이트를 변조하거나 혹은 악의적인 사이트로 사용자를 이동시킬 수 있다.

압수한 개인정보 파일을 추가 조사하는 과정에서 유출 사고를 인지하였으나, 유출신고를 해야 하는지 몰라 신고를 하지 않았다. 피심인은 중앙전파관리소 조사 시 신고절차 안내를 받고 2018.2.20. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 유출 신고를 하였으며, 이용자 통지에 대한 내부 회의를 거쳐 2018.3.7. 쇼핑몰 사업자(99개)의 사이트 관리자에게 유출사실에 대한 이용자 통지 안내를 하였다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보의 분실 · 도난 · 유출 사실{정보통신망법 제27조의3(개인정보 유출 등의 통지 · 신고)}**을 지연 신고한 행위**

피심인은 숙박앱 ‘ ’를 해킹한 해커 일당을 검거하여 수사 중이던 경찰청으로부터 연락을 받아 자사의 쇼핑몰 솔루션 서비스를 이용하는 사업자(99개사)가 운영 중인 쇼핑몰을 이용하는 이용자의 개인정보가 유출되었다는 사실을 2017.7.13. 인지하였다.

피심인은 개인정보 유출사실을 인지한 때(2017.7.13.)로부터 223일이 경과한 2018.02.20. 개인정보보호 포털(i-privacy.kr, KISA)에 신고하였다.

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

1) (안전한 인증수단) 피심인은 개인정보 유출 당시 이용자의 개인정보(성명, ID, 전화번호 등)를 열람 및 다운로드할 수 있는 개인정보처리시스템인 관리자페이지( )에 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 하였고, 2017.8월말 경부터 관리자페이지에 허용된 IP 주소만 접속이 가능하도록 설정하여 운영한 사실이 있다.

2) (침입탐지시스템의 설치·운영) 피심인은 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능이 있는 시스템을 설치·운영하지 않은 사실이 있다.

3) (최대 접속시간) 피심인은 개인정보취급자가 개인정보처리시스템(관리자페이지)에 접속한 후 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 접속이 차단되도록 최대 접속시간 제한 등의 조치를 하지 않은 사실이 있다.

다. 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. 8. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 " 유출등 "이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목(제1호)', '유출등이 발생한 시점(제2호)', '이용자가 취할 수 있는 조치(제3호)', '정보통신서비스 제공자등의 대응 조치(제4호)', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)'의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다." 라고 규정하고 있다.

정보통신망법 시행령 제14조의2제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호

의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다." 라고 규정하고 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)' 를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템(개인정보처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 의 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) 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다." 라고 규정하고 있다.

고시 제4조제5항은 "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 시스템

을 설치·운영하여야 한다." 라고 규정하고 있다.

고시 제4조제10항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다." 라고 규정하고 있다.

다. 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." 고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 분실·도난·유출 사실{정보통신망법 제27조의3(개인정보 유출 등의 통지·신고)}**을 지연 신고한 행위**

정보통신망법 제27조의3제1항의 '지체 없이' 에 대해서 정보통신망법에 별도로 규정된 정의는 없으나, 관련 판례에서는 '합리적인 이유 및 근거가 없는 한 즉시' 로 해석하고 있다.

따라서 피심인이 개인정보의 유출 사실을 안 때(2017.7.11.)로부터 223일이 경과한 2018.02.20.에 개인정보보호 종합포털(privacy.go.kr)에 신고한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

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

1) (안전한 인증수단) 고시 제4조제4항의 입법 목적은 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지

기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다는 것이다.

피심인이 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 별도의 안전한 인증수단(ex. 보안토큰, 휴대폰 인증 등) 없이 아이디와 비밀번호만으로 접속이 가능하게 한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

2) (침입탐지시스템의 설치·운영) 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(침입차단기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출 시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

피심인이 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 침입탐지시스템을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항제2호를 위반한 것이다.

3) (최대 접속시간) 고시 제4조제10항의 입법 취지는 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되도록 최대 접속시간 제한 등의 조치를 취하여야 한다는 것이다.

피심인이 개인정보취급자가 개인정보처리시스템(관리자페이지)에 접속한 후 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 접속이 차단되도록 최대 접속시간 제한 등의 조치를 하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

〈참고 5〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	지연 신고	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②5호	개인정보취급자의 접속시간이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하지 않은 행위(고시§4⑩)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

3) 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취할 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.

3. 과태료 부과

피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제2호의3·제3호, 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 각 적용한다.

〈참고 6〉 위반 횟수별 과태료 금액

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
하. 법 제27조의3제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조 제1항제2호의3	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

나. 과태료의 가중·감경

특별히 과태료를 가중·감경할 사유가 없어 기준금액을 유지한다.

〈참고 7〉 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§27의3①	1,000만원	없음	없음	**1,000만원**
§28①2호	1,000만원	없음	없음	**1,000만원**
계				**2,000만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제27조의3제1항, 제28조제1항 위반행위에 대해 2,000만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제2호의3·제3호에 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)