

방 송 통 신 위 원 회

심의 · 의결

안건번호 제2017 - 36 - 216호

안 건 명 개인정보 유출신고 사업자 등의 개인정보보호 법규 위반에 대한
시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2017. 10. 12.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 ①개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치의 설치·운영, ②외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용, ③개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 수시로 인터넷 홈페이지 취약점을 점검하는 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 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

- 가. 과 태 료 : 15,000,000원
- 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 온라인 등으로 위생도기를 제조·판매하는 웹사이트를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공이고, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

구 분	2014년	2015년	2016년	평 균
매출액(단위 : 백만원)				

※ 자료 출처 : 피심인이 제출한 자료



II. 사실조사 결과

1. 조사 대상

방송통신위원회는 이용자 6,159명에게 스미싱 문자가 발송되어 개인정보 유출이 의심된다는 개인정보 유출신고(2017. 6. 6.)가 개인정보보호 포털(i-privacy.kr, KISA)에 접수됨에 따라, 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사(2017. 6. 15.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위

(안전한 인증수단) 피심인은 이용자의 개인정보를 보관·처리하고 있는 개인정보처리시스템인 관리자 사이트)를 운영하고 있으며, 개인정보취급자가 정보통신망을 통해 외부에서 동 개인정보처리시스템에 접속하는 경우 2017. 6. 5. 휴대전화 인증수단을 시행하기 이전까지는 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 하였다.

(침입차단시스템 및 침입탐지시스템의 설치·운영) 피심인은 2017. 6. 6.부터 개인정보처리시스템에 대한 접속 권한을 IP로 제한적용하고 2017. 8. 4.부터 웹 방화벽을 설치·운영하기 전까지 방화벽 및 침입탐지시스템 등 접근통제장치를 설치·운영하지 않아, 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 차단하지 않았고 개인정보처리시스템에 접속한 IP 등을 재분석하여 불접적인 개인정보 유출 시도를 탐지하지 않았다.

(웹페이지 취약점) 피심인은 웹사이트

를 운영하면서 취급 중인



개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 웹 취약점 점검 등의 조치를 취한 사실이 없다.

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2017. 7. 24. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청 하였으며, 피심인은 2017. 8. 8. 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)’ 등의 기술적·관리적 조치를 하여야 한다.”라고 규정하고 있다.

나. 정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템(이하 “개인정보처리시스템”이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’, ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’를 하여야 한다.”라고 규정하고 있다.

다. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위



원회 고시 제2015-3호, 이하 ‘고시’) 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”라고 규정하고 있으며,

고시 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’하는 기능, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’하는 기능을 포함한 시스템을 설치·운영하여야 한다.”라고,

고시 제4조제9항은 “정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

라. 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 하고 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호



조치 중 접근통제), 시행령 제15조제2항제1호, 고시 제4조제4항을 위반하였고,

개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 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·운영하지 않고, 개인정보 파일이 외부로 유출되는 것을 탐지하도록 IP주소 등을 재분석하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제2호, 고시 제4조제5항을 위반하였고,

개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제5호, 고시 제4조제9항을 위반하였다

〈참고〉 피심인의 위반사항

사업자 명	위 반 내 용	법령 근거		
		법률	시행령	세부내용(고시 등)
	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	취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 인터넷 홈페이지에 취약점 점검을 하지 아니한 행위(고시§4⑨)



IV. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 ①외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용, ②개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치의 설치·운영, ③개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 수시로 인터넷 홈페이지 취약점을 점검 등 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 하는 등 기술적·관리적 보호 조치를 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 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 과태료 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과태료는 같은 법 제76조제1항제3호, 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 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
○ 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 행위가 2개 이상에 해당하므로, 기준금액의 50%를 가중한다.

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 위반행위가 과실에 의한 것이라 볼 수 없고, 피심인의 사업규모 등을 고려하여 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28①2호	1,000만원	500	없음	1,500만원
계				1,500만원

다. 최종 과태료

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

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항 및 제76조제1항 제3호에 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」 제 20조 규정에 의하여 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 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.

위원장

이 효 성



부위원장

허 욱



위원

김 석 진



위원

표 철 수



위원

고 삼 석

