방 송 통 신 위 원 회
심의·의결

안건번호 제2019 - 41 - 195호

안 건 명 등 50개사 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2019. 8. 23.

주 문

1. 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. 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·운영하여야 할 것

나. 개인정보처리시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 할 것

다. 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장할 것

2. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

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 : 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

(이하 '피심인'이라 한다)는 영리를 목적으로 프린터, 잉크 등 사무용품 판매 사이트　　를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표자	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 백만원)

구 분	2015년	2016년	2017년	평균
매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 서울동부지방검찰청으로부터 개인정보 유출 사업자를 통보받아 피심인을 대상으로 정보통신망법 위반여부에 대한 개인정보 취급·운영 실태를 현장조사(2018. 6. 26., 7. 3.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 프린터, 잉크 판매 사이트 를 운영하면서 2018. 6. 26. 기준 건의 회원정보를 수집·보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구 분	항 목	수집일	건수
이용자 정보	이름, 아이디, 비밀번호, 이동전화번호, 전화번호, 생년월일, 이메일주소, 주소		

나. 개인정보 유출 규모 및 경로

(1) **개인정보 유출 규모**

피심인이 프린터, 잉크 판매 사이트를 운영하면서 수집한 회원의 개인정보 90,393건이 유출되었다.

< 피심인의 개인정보 유출 현황 >

구분	유 출 항 목	건 수
회원	아이디, 이메일, 일반전화번호, 휴대전화전호	90,393건

(2) **유출 경로**

미상의 해커가 2017. 9. 1. SqlMap 툴을 사용하여 SQL Injection 방법으로 피심인의 쇼핑몰 사이트를 공격하여 피심인의 이용자 개인정보가 유출되었다.

(3) **유출 인지 및 대응**

피심인은 2018. 3. 13. 한국인터넷진흥원으로부터 받은 개인정보 유출관련 이메일을 2018. 3. 18. 확인 후 유출을 인지하였고, 2018. 3. 19. 한국인터넷진흥원에 개인정보 유출사실을 신고하였으며, 2018. 6. 26. 회원정보가 담긴 파일을 전달받아 2018. 6. 27. 이용자에게 개인정보 유출사실을 이메일로 통지하였다.

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 정보통신망을 통한 불법적인 접근을 차단하기 위한 침입차단시스템 및 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 시스템을 설치·운영하지 않은 사실이 있다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) **중 접속기록의 위·변조방지}을 소홀히 한 행위**

피심인은 현장조사일인 2018. 6. 26. 현재 개인정보처리시스템의 관리자페이지에 접속한 기록을 보관하지 않은 사실이 있다.

다. 개인정보의 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인은 이용자 95,545명의 비밀번호를 안전하지 않은 암호화방식(MD5)으로 데이터베이스에 저장한 사실이 있다.

라. 서비스를 이용하지 않은 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

피심인은 운영 중인 홈페이지 이용자의 개인정보 95,545건을 보관하면서 1년 동안 로그인 기록이 없는 이용자의 정보를 파기하거나 또는 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 9. 18. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 10. 2. 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)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)'의 조치를 하여야 한다."라고 규정하고 있고, 제3항은 "정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)'의 조치를 하여야 한다."라고 규정하고 있으며, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)' 등을 하여야 한다."라고 규정하고 있고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적 기준을 정하여 고시하여야 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 한다라 한다) 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)'의 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있다.

고시 제5조제1항은 "개인정보취급자가 개인정보 처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있다.

고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 아이디 등), 접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점) 〈년-월-일, 시:분:초〉, 접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), 수행업무(개인정보처리시스템에서 개인정보취급자가 처리한 내용을 알 수 있는 정보) 〈개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위〉 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다고 해설하고 있다.

고시 제6조제1항에 대해 정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조 되지 않도록 개인정보처리시스템, 업무용컴퓨터, 보조저장매체 등에 일방향 암호화(해쉬함수 적용)하여 저장하여야 하며 무작위 대입공격(Brute Force), 레인보우 테이블 공격 등을 이용한 비밀번호 복호화에 대응하기 위하여 난수추가(salting) 등의 조치를 하여야 하며 국내·외

암호 연구 관련 기관에서 사용 권고하는 안전한 암호 알고리듬으로 암호화하여 저장하고, 보안강도가 낮은 것으로 판명된 암호 알고리듬(MD5, SHA-1 등)을 사용해서는 안된다고 해설하고 있다.

나. 정보통신망법 제29조제2항은 "정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제16조제2항은 "정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다."라고 규정하고 있다.

다. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 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**

피심인이 정보통신망을 통한 불법적인 접근을 차단하기 위한 침입차단시스템 및 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 시스템을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인이 현장조사일(2018. 6. 26.) 현재 개인정보처리시스템의 관리자페이지에 접속한 기록을 보관하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

다. 개인정보의 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인이 이용자 95,545명의 비밀번호를 안전하지 않은 암호화방식(MD5)으로 데이터베이스에 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

라. 서비스를 이용하지 않은 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

피심인이 정보통신서비스를 1년의 기간 동안 이용하지 않은 이용자의 개인정보 95,545건을 파기하거나 또는 별도로 저장·관리하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 않은 행위(고시§4⑤)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월 1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 않은 행위(고시§5①)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 일방향 암호화하여 저장하지 않은 행위(고시§6①)
	유효 기간	§29②	§16②	1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 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) 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·운영하여야 할 것 2) 개인정보처리시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 할 것 3) 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장할 것

나. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 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 및 제29조(개인정보의 파기)제2항 위반에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 같은 법 시행

령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 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.

〈 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
더. 법 제29조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조 제1항제4호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위가 3개에 해당하는 경우이므로 기준금액의 100분의 50인 500만원을 가중한다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

위반의 정도	가. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내
	제3호 정보통신망법 시행령 제74조별표 9 제2호 너목 가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행을 하지 않은 경우 나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우 다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우 라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우 마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치를 하지 않은 경우 바. 정보통신망법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하지 않은 경우	

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

그러나 피심인의 정보통신망법 제28조제1항 및 제29조제2항 위반행위에 대해서 특별히 해당사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2·3·4호	1,000만원	500만원	없음	**1,500만원**
§29②	1,000만원	없음	없음	**1,000만원**
계				**2,500만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 및 제29조제2항 위반행위에 대해 2,500만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호·제4호(과태료)에 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.

이에 주문과 같이 의결한다.

2019년 8월 23일

위 원 장　　이 효 성 (인)

부위원장　　김 석 진 (인)

위　　원　　허　　욱 (인)

위　　원　　표 철 수 (인)

위　　원　　고 삼 석 (인)