방 송 통 신 위 원 회
심의 · 의결

안건번호 제2019 - 44 - 260호

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

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2019. 9. 6.

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·운영할 것

나. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

2. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날로부터 1개월이내에 4단×10㎝ 또는 5단×9㎝의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 앱에 1주일 이상 게시하여야 한다. 이때, 공표 내용 등은 방송통신위원회와 사전 협의를 거쳐야 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 과징금 및 과태료를 부과한다.

가. 과 징 금 : 18,900,000원

나. 과 태 료 : 10,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

마. 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 온라인으로 쇼핑몰 솔루션 개발 및 임대 등 서비스를 제공하기 위해 웹사이트 를 운영하는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표자	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 백만원)

구 분	2014년	2015년	2016년	평균
매출액				
정보통신서비스				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 2018. 3. 5. 서울동부지방검찰청으로부터 피심인의 솔루션을 이용하는 정보통신서비스 제공사업자의 이용자 개인정보가 미상의 해커(이하 '해커'라 한다)에 의해 유출되었다고 전달받았고 이에, 한국인터넷진흥원과 함께 피심인에 대한 정보통신망법 위반 여부를 확인하기 위해 개인정보 처리·운영 실태를 조사(2018. 8. 30. ~ 8. 31. / 9. 11.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

1) 서비스 제공 현황

피심인은 쇼핑몰 솔루션 개발 및 임대 등 사업을 하면서 2018. 8. 31. 현재 아래와 같이 서비스를 제공하고 있으며 e나무 임대형을 이용하는 정보통신서비스 제공사업자와는 위·수탁 관계가 있다.

구분	서비스명	개시일	가격	이용자 수
단독형				
임대형				

나. 개인정보 유출 규모 및 경로

피심인의 쇼핑몰 솔루션 을 구매 또는 임대하여 사용하는 43개 정보통신서비스 제공자의 서비스를 이용하는 회원의 개인정보(아이디, 비밀번호, 이메일, 전화번호, 휴대전화번호) 3,220,666건(임대형 : 110,795건, 독립형 : 3,109,871건)이 유출되었다.

- 각 정보통신서비스 제공자별 상세 개인정보 유출규모는 아래와 같다.

사업자명	유출시기	유출건수	유출항목
	'17.9.15	10,007	아이디,이메일,일반전화,휴대전화
	'17.9.13., 19.	120,299	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.18	30,835	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.21	15,056	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	69,344	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.12	57,353	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.13	18,035	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.20	290,873	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.13.	18,054	아이디,이메일,일반전화,휴대전화
	'17.9.17	973,634	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19.	36,914	아이디,이메일,일반전화,휴대전화
	'17.9.18	11,886	비밀번호,아이디,이메일,휴대전화
	'17.9.13	48,512	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.12., 14.	100,951	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.12	43,111	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.15	61,802	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	17,674	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.13	31,430	비밀번호,아이디,이메일,일반전화,휴대전화

사업자명	유출시기	유출건수	유출항목
	'17.9.12	7,570	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	141,697	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	26,504	아이디,이메일,일반전화,휴대전화
	'17.9.19	24,324	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.13	20,922	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.1	3,014	비밀번호,아이디,이메일,휴대전화
	'17.9.15	17,674	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	12,205	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.18	35,879	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.15.	14,630	아이디,이메일,일반전화,휴대전화
	'17.9.12	56,120	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	10,419	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.12	4,278	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	41,587	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.15.~16., 20.	101,866	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.12	268,615	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.15.	17,844	아이디,이메일,일반전화,휴대전화
	'17.9.12	21,916	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.13.,9.21.	147,393	아이디,이메일,일반전화,휴대전화
	'17.9.14., 19	28,676	비밀번호,아이디,이메일,휴대전화
	'17.9.12	98,492	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.19	20,214	아이디,이메일,일반전화,휴대전화
	'17.9.13	12,030	비밀번호,아이디,이메일,휴대전화
	'17.9.15	97,011	비밀번호,아이디,이메일,일반전화,휴대전화
	'17.9.18	34,016	아이디,이메일,일반전화,휴대전화

(2) 유출 경로

이 사건 해커는 2017. 9. 12.부터 9. 21.까지 총 5개의 서버[호스팅업체 및 IP : (27.255.), (14.49.), (117.52.), (118.217.), (112.175.)]에 직접 접속하거나 경유 서버를 통해 43개 정보통신서비스 제공사업자의 홈페이지에 대한 SQL Injection 공격 방식으로 회원DB 정보를 탈취하였다.

※ SQLMap 도구를 이용하여 특정 웹페이지(, 온라인 쇼핑몰의 상품 구매 웹페이지)의 공개된 소스코드 중 SQL 취약점을 공격

(3) 유출사고 인지

2017. 9. 19. 22:08 피심인은 보안관제 담당자 (, 홍○○)로부터 '[ ][SOC][침해분석] 공인 IP 할당(106.249.) Critical_SQL_Injection' 이란 메일을 받고 피심인의 쇼핑몰 솔루션을 이용한 의 개인정보가 유출된 것을 확인하면서 를 이용하는 43개사에 대한 해킹사고 발생 사실을 인지하였으며, 2017. 9. 21. 피심인은 유출사고 관련 보안패치를 배포하였다.

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**

1) (침입차단 및 탐지시스템 설치·운영) 피심인은 이 사건 당시 개인정보처리시스템에 대한 불법적인 침입 차단 및 탐지를 위해 방화벽과 IDS를 설치하여 와 을 통해 IDS에 대한 보안관제 서비스를 받고 있었으나, 개인정보 유출사고가 발생한 총 43개 홈페이지 중 16개(12개, 4개) 홈페이지만 보안관제가 이루어지고 나머지 27개 홈페이지에 대해서는 실질적으로 침입차단 및 탐지시스템이 정상적으로 운영되지 않은 사실이 있다.

는 유출사고가 발생하기 이전에 관제 대상인 12개 홈페이지 중 9개 홈페이지에 대해서 SQL Injection 공격 시도를 탐지하고 피심인에게 해당 사실을 보고[1]하였으나 피심인은 이와 관련하여 어떠한 조치도 취하지 않은 사실이 있다.

1) 는 피심인이 운영하는 IDS로그를 ESM(Enterprise Security Management, 보안장비)으로수집하여 보안 이벤트(5가지 유형)가 탐지되는 경우, 실제 공격의 일부 패킷을 캡처하여 해당 패킷에서 발생되는 공격 구문과 동일한 공격을 수행하며 이를 통해 도출된 공격 영향도(공격의 성공 여부)를 분석하여 피심인에게 보고하고 있음

방송통신위원회는 피심인이 침입차단 및 탐지시스템을 적정한 수단과 방법으로 설치·운영하고 있었는지 확인할 목적으로 개인정보가 유출된 43개 홈페이지에 대한 해킹사고 관련 탐지로그 분석결과 및 대응보고서 등을 제출할 것을 요청('19.6.24.)하였으나, 피심인은 1개 홈페이지(2017.9.19.)를 제외하고 관련 자료를 제출하지 못하였으며 처분의 원인인 해킹사고와 직접적으로 관련이 없는 자료(취약점 점검, 개발보안 가이드라인 등)만 제출('19.6.19.)한 바 있다.

2) **(열람권한이 없는 자에게 유출)** 피심인은 솔루션에서 발생 가능한 공격에 대응하기 위해 보안 코딩을 적용하였고, 신규 위협에도 대응하기 위해 모의해킹과 같은 취약점을 진단하고 개선조치를 이행해 왔다고 주장하나,

피심인이 제출한 취약점 점검사항은 해킹사고의 원인이 된 '온라인 상품구매 페이지 '에 대한 취약점 점검을 했다는 증빙자료가 아니며, 조사 당시 확인한 결과, 해당 페이지는 SQL Injection 공격을 막기 위한 구문 삽입 등 기본적인 조치조차 이루어지지 않은 상태였다.

<참고 : 온라인 상품구매 페이지 소스코드 화면>

피심인은 유출사고가 발생한 이후 업데이트 패치 배포(2017.9.19.~21.)를 통해 해킹사고 관련 페이지 에 대한 SQL 취약점을 개선한 것이 확인되므로 개인정보 유출 방지를 위한 최대한의 조치를 이행하였다고 보기 어렵다.

따라서 피심인의 쇼핑몰 솔루션 을 구매 또는 임대하여 사용하는 43개 정보통신서비스 제공자의 이용자 개인정보가 알 수 없는 해커의 SQL Injection 공격에 의해 2017. 9. 12. ~ 9. 21. 사이 3,220,666건이 열람권한이 없는 자에게 유출되었다.

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2019. 5. 27. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 6. 19. 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)'을 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

(제5호)'를 하여야 한다."라고 규정하고 있고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 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 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)'하는 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있고, 제9항은 "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.

'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, 보안운영체제(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.

또 고시 제4조제9항에 대해 아래와 같이 해설하고 있다.

첫째, 인터넷 홈페이지 설계 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 1) 입력 데이터의 유효성 검증, 2) 인증, 접근통제 등의 보호조치 적용, 3) 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성, 4)세션을 안전하게 관리하도록 구성하는 등 보안대책을 마련하여야 한다는 것이다.

둘째, 인터넷 홈페이지 개발 시 개인정보 유·노출 방지를 위해 1) 홈페이지 주소(URL), 소스코드, 임시저장 페이지 등에 개인정보 사용금지, 2) 홈페이지에 관리자 페이지의 주소링크 생성금지, 관리자 페이지 주소는 쉽게 추측하기 어렵도록 생성, 관리자 페이지 노출금지, 3) 엑셀파일 등 숨기기 기능에 의한 개인정보 유·노출 금지, 4) 시큐어 코딩(입력데이터 검증 및 표현<SQL 삽입 등>, 보안기능<부적절한 인가 등>, 시간 및 상태<종료되지 않는 반복문 등>, 에러처리<오류상황 대응 부재 등>, 코드오류<해제된 자원 사용>, 캡슐화<잘못된 세션에 의한 정보 노출>, API 오용<취약한 API 사용 등>) 등 도입, 5)취약점을 점검하고 그 결과에 따른 적절한 개선 조치, 6)인증 우회(authentication bypass)에 대비하는 조치 등 보안기술을 적용하여야 한다는 것이다.

셋째, 인터넷 홈페이지 운영 관리 시 1)보안대책을 정기적으로 검토, 2)홈페이지 게시글, 첨부파일 등에 개인정보 포함 금지, 정기적 점검 및 삭제 등의 조치, 3) 서비스 중단 또는 관리되지 않는 홈페이지는 전체삭제 또는 차단조치, 4) 공격패턴, 위험분석, 침투 테스트, 등을 수행하고 발견되는 결함에 따른 개선 조치, 5) 취약점을 점검(취약점 점검 시에는 기록을 남겨 추적성 확보 및 향후 개선조치 등에 활용할 수 있도록 할 필요가 있으며 정기적으로 웹셸 등을 점검하고 조치한다면 취급중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다)하고 그 결과에 따른 적절한 개선조치 등 개인정보 유·노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선조치를 하여야 한다는 것이다.

나. 정보통신망법 제64조제3항은 “방송통신위원회는 정보통신서비스 제공자등

이 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

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

1) (침입차단 및 탐지시스템 설치·운영) 가 유출사고 이전에 SQL Injection 공격 시도를 탐지하고 피심인에게 보고한 9개 홈페이지 중에는 피심인이 임대형으로 서비스를 제공하고 있는 5개사 중 3개사의 홈페이지도 포함되어 있었으나, 피심인이 의 이상 행위 탐지 보고에 대해 IP 차단 요청, 초동 분석 결과 검증 등의 어떠한 대응 조치도 취하지 않은 사실은 침입차단 및 탐지시스템을 정상적으로 운영하지 않았다는 것을 의미한다. 만약 피심인이 가 보고한 이상 행위에 대해 시의 적절하게 대응하였다면 금번 개인정보 유출사고 발생을 사전에 차단하였거나 유출피해를 최소화 할 수 있었을 것으로 판단된다.

따라서 피심인이 해커의 침입을 탐지(SQL Injection 공격 시도)하였음에도 불구하고 침입행위에 대한 분석 및 차단 등의 조치를 취하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

2) (열람권한이 없는 자에게 유출) 피심인이 쇼핑몰 솔루션 이하)을 임대하여 사용하는 등 5개 정보통신서비스 제공자의 이용자 개인정보가 알 수 없는 해커의 SQL Injection 공격에 의해 열람권한이 없는 자에게 유출되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항5호, 고시 제4조제9항을 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)
	접근 통제	§28①2호	§15②5호	개인정보가 열람권한이 없는 자에게 공개·유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

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·운영할 것 2) 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

나. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날로부터 1개월이내에 4단×10㎝ 또는 5단×9㎝의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 어플리케이션에 1주일 이상 게시하여야 한다. 이때, 공표 내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

< 시정명령 공표(안) 예시 >

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ① 개인정보의 안전성을 확보하기 위하여 침입차단 및 탐지시스템을 설치·운영하지 않은 행위, ②개인정보가 열람권한이 없는 자에게 노출되지 않도록 조치하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

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.

V. 과징금 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 〔별표 8〕 (과징금의 산정기준과 산정절차) 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(방송통신위원회 고시 제2015-30호, 이하 '과징금 부과기준'이라 한다)' 따라 다음과 같이 부과한다.

1. 과징금 상한액과 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 상한액은 같은 법 제64조3의제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신

서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

과징금 부과기준 제5조제1항은, 정보통신망법 시행령 〔별표 8〕 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따라, 피심인은 영리를 목적으로 온라인 쇼핑몰 솔수션 개발 및 임대하는 정보통신서비스 제공자로서 ▲정보통신망법 제28조제1항제2호에 따른 접근통제 중 기술적·관리적 보호조치 중 개인정보처리시스템에 침입차단 및 침입탐지 시스템을 설치·운영하지 않은 행위, ▲개정보통신망법 제28조제1항제2호에 따른 개인정보가 열람권한이 없는 자에게 공개·유출되지 않도록 조치를 취하지 않은 행위 등으로 미상의 해커에 의해 5개 임대형사업자 이용자의 개인정보가 유출되게 하는 빌미를 제공하였으므로 피심인에게 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있고,

과징금 부과기준 제5조제3항 단서조항은, 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가

공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 규정하고 있다.

이에 따라, 피심인의 위반행위의 결과가 ▲개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점, ▲유출된 개인정보가 5개 임대형사업자가 보유하고 있는 개인정보의 100분의 5 이상(2018. 8. 기준, 5개 임대형사업자의 개인정보 건 중 110,795건 유출)인 점, ▲이용자의 개인정보가 공중에 유출된 점 등을 종합적으로 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 임대형 쇼핑몰사업자의 임대료수익을 위반행위와 관련 매출로 하고, 위반행위 직전 3개 사업년도의 연평균 매출액 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 으로 한다.[2)]

< 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 부과기준율 >

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 위반행위의 기간이 1년 이내('17.9.12.~'17.9.21.)이므로 기준금액을 유지하고,

2) 제2019-41차 회의('19.8.23.) 시 착오에 의해 위반행위와 관련한 매출액을 '15년~'17년의 연평균 매출액으로 산정하였으나, 제2019-44차 회의('19.9.6.)에서 피심인의 위반행위 직전 3개 사업연도인 '14년~'16년의 연평균 매출액으로 산정하는 것으로 수정 의결함

최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 원을 감경한 원으로 한다.

라. 추가적 가중 및 감경

특별히 추가적으로 가중할 사항은 없으며, 방송통신위원회의 조사에 적극 협력한 점을 고려하여 100분의 20인 원을 감경한다.

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 과징금부 과기준에 따라 위와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 미만에 해당하여 십만원 미만을 절사한 18,900,000원을 최종 과징금으로 결정한다.

< 과징금 산출내역 >

기준금액	필수적 가중감경	추가적 가중감경	**최종 과징금***
원	필수적 가중 없음 필수적 감경 (50%, 원)	추가적 가중 없음 추가적 감경 (20%, 원)	**18,900천원**
	→ 원	→ 원	

* '전기통신사업법 금지행위 위반에 대한 과징금 산정 실무요령'에 따라 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

VI. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는

같은 법 제76조제1항제3호, 같은 법 시행령 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 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

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보 제공 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.

그러나 피심인의 정보통신망법 제28조제1항 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 가중하지 않는다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자

금사정, ▲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 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

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

다. 최종 과태료

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

< 위반행위별 과징금 · 과태료와 시정명령 >

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2호	**1,890만원**	**1,000만원**	O	**2,890만원**

Ⅶ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제3호(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 9월 6일

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)