방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 09 - 060호

안 건 명 개인정보보호 법규 위반한 12개사에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 2. 21.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ① 개인정보보호 조직의 구성 및 운영에 관한 사항과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 정기적인 교육에 관한 사항을 포함하여 개인정보 안전성 확보를 위하여 필요한 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성프로그램 방지, 출력·복사 시 보호조치) 이행을 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행하여야 하며, ②개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, ③개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관하여야 하며, ④외부에서 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 적용하여야 하며, ⑤정보통신망을 통해 개인정보처리시스템에 불법적인 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ⑥개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하여야 하며, ⑦비밀번호는 복호화 되지 아니하도록 일방향 암호화(해쉬함수, 128비트 이상 보안강도)하여 저장하여야 하며, ⑧이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ⑨정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 한다.

2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시결과를 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 전기통신사업자의 전기통신역무를 이용하여 증권 강좌 웹사이트( )를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이다.

피심인은 부터 동 웹사이트( )를 운영하면서 이용자의 개인정보를 수집·이용하여 2017. 9. 12. 현재 명의 회원의 개인정보(이름, 닉네임, 아이디, 비밀번호, 연락처, 생년월일, 이메일 주소 등)를 수집·이용하고 있으며, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

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

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사대상

방송통신위원회는 해킹에 의해 회원 명의 개인정보가 유출되었다는 피심인의 유출신고가 개인정보보호 포털(i-privacy.kr, KISA)에 접수(2017.8.11.)됨에 따라, 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2017.9.11.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 개인정보 내부관리계획을 수립·시행하지 아니한 행위

피심인은 개인정보보호 조직의 구성 및 운영에 관한 사항과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 정기적인 교육에 관한 사항을 포함하여 개인정보를 안전하게 처리하기 위한 내부 관리계획을 수립·시행하지 않았다.

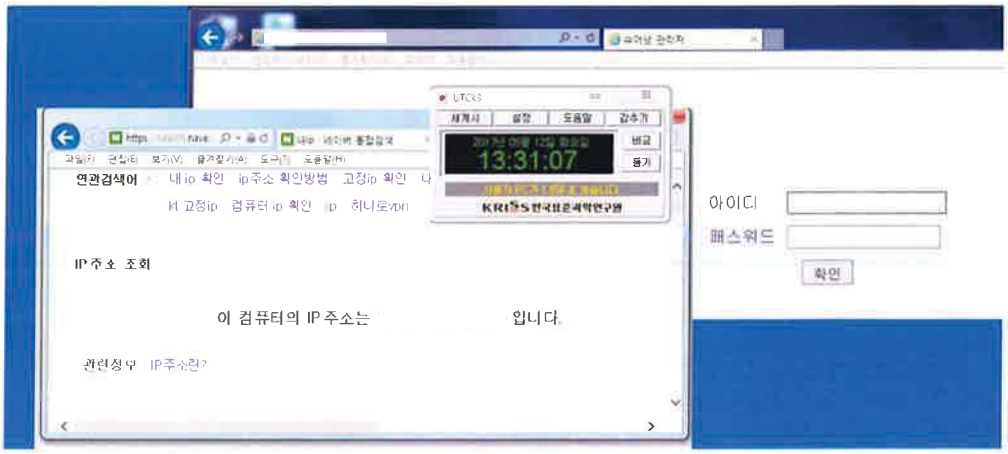
나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

(접근권한 부여·말소) 피심인은 이용자의 개인정보를 처리할 수 있도록 구성된 개인정보처리시스템( )을 운영하고 있으며, 개인정보취급자(7명)가 아님에도 불구하고 퇴직자(1명)에게 개인정보처리시스템에 대한 접근권한을 부여하고 있었다.

(접근권한 기록보관) 피심인은 개인정보처리시스템( )에 대하여 개인정보관리책임자 및 개인정보취급자의 접근 권한 부여 및 변경 또는 말소에 관한 내역을 기록하여 보관하지 않았다.

(안전한 인증수단) 피심인은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템( )에 접속하는 경우 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 하였다.

<참고 1> 외부에서 개인정보처리시스템 접속시 안전한 인증수단 미적용



(침입차단시스템 및 침입탐지시스템의 설치·운영) 피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근 제한 기능 및 유출 탐지 기능이 포함된 접근통제장치를 설치·운영하지 않았다.

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

피심인은 개인정보취급자가 개인정보처리시스템의 관리자페이지에 접속한 기록은 2017. 9. 4.부터 기록하여 보관하고 있으며, DB에 접속한 내역은 기록하여 보관하지 않았다.

라. 개인정보의 암호화를 소홀히 한 행위

(비밀번호 암호화) 피심인은 이용자 명의 비밀번호를 저장하면서 양방향 암호화하여 저장하였다.

<참고 2>이용자의 비밀번호를 복호화 한 화면

mid	userid	userpw	username	nick	email	phone	mobile	sms_receive
20699	hbc7538	h150	한 찬	윤	0		0102 38	1
20698	iydh62	dh20	유 훈	iy	0		0109 03	0
20697	seedkyn	song	김 남	프	0		0109 81	0
20696	africa5325	afric	박 희	하	0		0107 95	1
20695	overdream	ygyk	남 근	꿈	0		0103 07	0
20694	kimrich7	kim	김 형	김	0		0108 59	1
20693	rhfoddl2	wpf	고 혁	슈	0		0108 12	1

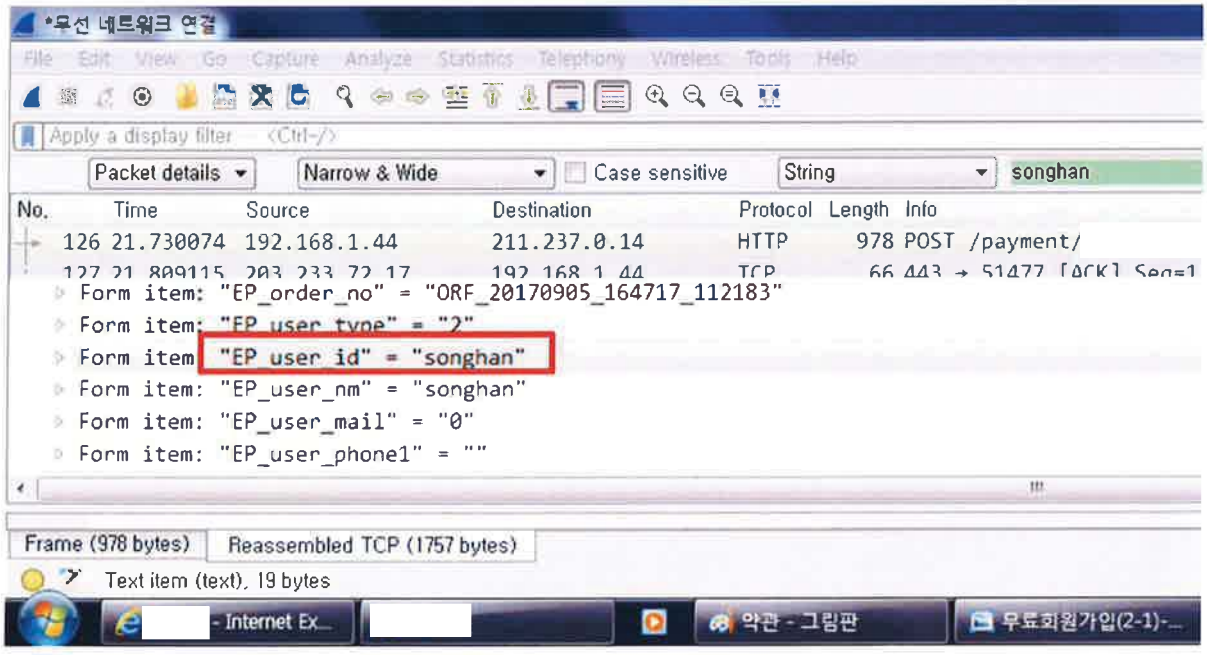
(계좌번호 암호화) 피심인은 이용자의 환불 계좌번호 건을 암호화하지 않고 평문으로 DB에 저장하였다.

<참고 3> 이용자의 계좌번호를 평문으로 DB에 저장

(전송구간 암호화) 피심인은 충전하기 웹페이지(

)에서 개인정보 및 인증정보를 송·수신 할 때 암호화 하지 않고 평문으로 이를 전송하였다.

<참고 4> 개인정보 송·수신 시 전송구간 미 암호화



마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2017. 12. 20. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴'' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 1. 4. 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 '개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행(제1호)', '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)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제1항은 "정보통신서비스 제공자등은 개인정보의 안전한 처리를 위하여 '개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항(제1호)', '정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리하는자의 교육에 관한 사항(제2호)', '개인정보 보호조치를 이행하기 위하여 필요한 세부 사항(제3호)'의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다."라고 규정하고 있고,

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 등의 조치를 하여야 한다."라고 규정하고 있고,

정보통신망법 시행령 제15조제3항은 "정보통신서비스 제공자등은 접속기록의

위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)' 등의 조치를 하여야 한다."라고 규정하고 있으며,

정보통신망법 시행령 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)', '주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)', '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치(제3호)'를 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') 제3조제3항은 "개인정보보호 조직의 구성·운영과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 교육의 세부계획, 고시 제4조부터 제8조까지의 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성 프로그램의 방지, 물리적 접근 방지) 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다."라고 규정하고 있고,

고시 제4조제2항은 "정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다."라고 규정하고 있고,

고시 제4조제3항은 "정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다."라고 규정하고 있고,

고시 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증

수단을 적용하여야 한다."라고 규정하고 있고,

고시 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.

고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월1회 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 있고, 제2항은 "정보통신서비스 제공자등은 계좌번호 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다."라고 규정하고 있고, 제3항은 "정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."라고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제3조제3항에 대해 내부관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 사업자 또는 대표자에게 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알리고 이를 준수할 수 있도록 하여야 한다고 해설하고 있고,

고시 제4조제2항에 대해 정보통신서비스 제공자등은 개인정보취급자가 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 개인정보처리시스템에 사용자계정 등 접근권한의 변경·말소 등이 필요할 때에는 정당한 사유가 없는 한 즉시 조치하여야 하며, 불완전한 접근권한의 변경 또는 말소 조치로 인하여 정당한 권한이

없는 자가 개인정보처리시스템에 접근될 수 없도록 하여야 한다고 해설하고 있고,

고시 제4조제3항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 5년간 보관하여야 하며, 관리대장 등에는 신청자 정보, 신청 및 적용 일시, 승인자 및 발급자 정보, 신청 및 발급사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하여야 한다고 해설하고 있고,

고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있고,

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 접근제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있고,

고시 제5조제1항에 대해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록(정보주체 식별정보, 개인정보취급자 식별정보, 접속일시, 접속지 정보, 부여된 권한 유형에 따른 수행업무 등 포함)을 최소 6개월 이상 저장하고 이를 월 1회 이상 정기적으로 확

인·감독하여야 한다고 해설하고 있고,

고시 제6조제1항에 대해 개인정보취급자 및 이용자의 비밀번호가 노출 또는 위·변조되지 않도록 일방향 함수(해쉬함수, 128비트 보안강도 권고)를 이용하여 저장하여야 한다고 해설하고 있고,

고시 제6조제2항에 대해 개인정보 유·노출 시에 2차 피해가 발생할 확률이 높은 계좌번호 등에 대해서는 안전한 알고리즘(128비트 이상)으로 암호화하여 저장·관리해야 한다고 해설하고 있고,

고시 제6조제3항에 대해 정보통신서비스 제공자등은 이용자의 성명, 연락처 등의 개인정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, SSL(Secure Sockets Layer) 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화하여 전송하는 방식이며, 응용프로그램을 이용한 보안서버는 웹서버에 접속하여 보안 프로그램을 설치하여 이를 통해 개인정보를 암호화 전송하는 방식이라고 해설하고 있다.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 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. 개인정보 내부관리계획을 수립·시행하지 아니한 행위

피심인이 개인정보보호 조직의 구성·운영과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 교육의 세부계획, 고시 제4조부터 제8조까지의 보호조치

(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성 프로그램의 방지, 물리적 접근 방지) 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하지 않은 행위는 정보통신망법 제28조제1항제1호(기술적·관리적 보호조치 중 내부관리계획의 수립·시행), 시행령 제15조제1항, 고시 제3조제3항을 위반하였다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

(접근권한 부여·말소) 피심인이 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제1호, 고시 제4조제2항을 위반하였고,

(접근권한 기록보관) 피심인이 개인정보처리시스템에 대한 접근 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 5년간 보관하지 아니한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제1호, 고시 제4조제3항을 위반하였고,

(안전한 인증수단) 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 보호조치 중 접근통제), 시행령 제15조제2항제1호, 고시 제4조제4항을 위반하였고,

(침입차단시스템 및 침입탐지시스템의 설치·운영) 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 시스

템을 설치·운영하지 않고, 개인정보 파일이 외부로 유출되는 것을 탐지하도록 IP주소 등을 재분석하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제2호, 고시 제4조제5항을 위반하였다.

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

피심인은 개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하지 않고 시스템 이상 유무의 확인등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하지 않음으로써 정보통신망법 제28조제1항제3호(기술적·관리적 보호조치 중 접속기록), 시행령 제15조제3항제1호, 고시 제5조제1항을 위반하였다.

라. 개인정보 암호화를 소홀히 한 행위

(비밀번호 암호화) 피심인은 이용자의 비밀번호를 저장하면서 이를 복호화 되지 아니하도록 일방향 암호화(해쉬함수, 128비트 이상 보안강도)하여 저장하지 않음으로써, 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제1호, 고시 제6조제1항을 위반하였고,

(계좌번호 암호화) 피심인은 이용자의 계좌번호를 안전한 암호알고리즘으로 암호화하지 않고 평문으로 DB에 저장하여 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호, 고시 제6조제2항을 위반하였고,

(전송구간 암호화) 피심인은 웹서비에 SSL(Secure Socket layer) 인증서를 설치하거나 암호화 응용프로그램을 설치하지 않아 정보통신망을 통해 이용자의 개인정보를 암호화하여 송·수신할 때 이를 암호화하지 않음으로써 정보통신망법 제28조제1항제4호, 시행령 제15조제4항제3호, 고시 제6조제3항을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	내부관리계획	§28①1호	§15①	개인정보의 안전성 확보를 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행하지 아니한 행위(고시§3③)
	접근통제	§28①2호	§15②1호	퇴사한 개인정보취급자의 개인정보처리시스템 접근권한을 말소하지 아니한 행위(고시§4②)
	접근통제	§28①2호	§15②1호	개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	접근통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)
	접속기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 양방향 암호화하여 저장한 행위(고시§6①)
	암호화	§28①4호	§15④2호	이용자의 계좌번호 등에 대해 안전한 알고리즘으로 암호화 하지 않고 평문으로 DB에 저장한 행위(고시§6②)
	암호화	§28①4호	§15④3호	이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위(고시§6③)

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ① 개인정보보호 조직의 구성 및 운영에 관한 사항과 개인정보관리책임자 및 개인정보취급자를 대상으로 한 정기적인 교육에 관한 사항을 포함하여 개인정보 안전성 확보를 위하여 필요한 보호조치(접근통제, 접속기록의 위·변조 방지, 개인정보의 암호화, 악성프로그램 방지, 출력·복사 시 보호조치) 이행을 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행하여야 하며, ②개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, ③개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관하여야 하며, ④외부에서 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 적용하여야 하며, ⑤정보통신망을 통해 개인정보처리시스템에 불법적인 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ⑥개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하여야 하며, ⑦비밀번호는 복호화되지 아니하도록 일방향 암호화(해쉬함수, 128비트 이상 보안강도)하여 저장하여야 하며, ⑧이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ⑨정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 한다.

2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여

개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 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 '처리지침'이라 한다)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 〉

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)** '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 이상인 경우이므로 기준 금액의 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 정보통신망법 제28조제1항 위반 행위 대해서 특별히 해당사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28①1·2·3·4호	1,000만원	500만원	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(시정명령) 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 의하여 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조 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 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)