방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 22 - 132호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사 :

의 결 일 2017. 8. 8.

주 문

1. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등 접근 통제장치의 설치·운영 및 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 이용자의 개인정보를 보호하기 위한 기술적·관리적 보호조치를 하여야 하고, 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 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 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제25조에 따라 전기통신사업자로부터 개인정보 처리 위탁을 받은 자로서 같은 법 제67조제2항에 따라 제28조, 제29조 등 개인정보 보호규정을 준용하는 사업자로, 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. 조사대상

방송통신위원회·행정자치부는 개인정보 관리 취약분야인 통신사 판매점을 대상으로 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 공동 기획조사(2017.2.7.~2017.2.8.) 하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위(정보통신망법 제28조제1항)

(1) 피심인은 외부에서 개인정보처리시스템 에 접속 시 단순히 아이디와 비밀번호만으로 접속이 가능하도록 하여 안전한 인증수단을 적용하지 않았다.

(2) 피심인은 개인정보처리자가 개인정보처리시스템 에 접속 시, 숫자만으로 구성된 4자리의 비밀번호만으로도 접속이 가능하도록 하여 비밀번호의 생성 방법 및 변경주기 등의 기준을 설정·운영하지 않았다.

(3) 피심인은 개인정보처리시스템 및 개인정보취급자의 컴퓨터 및 모바일기기에 조치를 취하지 않아, 열람권한 없는 자가 신분증, 가입신청서 등 이용자의 개인정보를 다운로드 가능 하도록 하였다

(4) 피심인은 모바일 관리시스템 D/B에 비밀번호 저장 시, 이를 암호화하지 않고 평문으로 저장 하였다.

(5) 피심인은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않았다.

(6) 피심인은 이용자의 개인정보 파일 2,313건을 개인용 컴퓨터에 저장할 때에 암호화하지 않고 저장하였다.

나. 개인정보를 파기하지 않은 행위(정보통신망법 제29조제1항)

피심인은 이동전화 개통 업무를 수행하면서 '12.2.21.부터 수집한 통신3사의

이용자 가입신청서 원본 및 사본 4,300여건을 사무실 내 캐비넷, 박스 등에 보관하였으며, 2010.6.5.부터 개인정보처리시스템 내 가입신청서 및 구비서류 등 개인정보 16,224건을 저장하여 개인정보의 보유 및 이용기간이 끝난 이용자 개인정보 총 20,524건을 2017.2.7. 조사 당시까지 파기하지 아니하고 보유하였다.

또한, 신청자의 주민등록번호, 여권번호 등이 포함된 신분증 사본 수건을 파기하지 않고 웹서버에 저장하여 수집하였다.

다. 사전통지 및 의견수렴

방송통신위원회는 2017. 4. 19. '개인정보보호 법규 위반사업자 사전통지 및 의견수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2017. 5. 16. 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 접근통제장치의 설치·운영(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등(제4호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)' 등의 조치를 하여야 한다."라고 규정하고 있고,

비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영(제4호), 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호) 등의 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') 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있으며

고시 제4조제8항은 "정보통신서비스 제공자등은 개인정보취급자를 대상으로 개인정보에 대한 불법적인 접근을 차단하기 위한 비밀번호 작성규칙을 수립하고, 이행한다."라고 규정하고 있다

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

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

고시 제6조제3항은 "정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능이나 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능 중 하나의 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."라고 규정하고 있다.

고시 제6조제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 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 필요하다"라고 해설하고 있다.

고시 제4조제8항에 대해 "비밀번호는 산업스파이, 침입자, 비인가자가 추측하기 어려운 문자와 숫자를 포함 하거나, 전에 사용된 비밀번호를 다시 사용하지 않는 등의 비밀번호 설정 원칙을 참고하여 생성하도록 한다"라고 해설하고 있다.

고시 제4조제9항에 대해 "개인정보취급자의 부주의로 고객 개인정보가 인터넷 홈페이지 또는 P2P를 통해 게시되거나, 공유 설정된 PC 폴더에 고객명단 파일을 둠으로써 열람 권한이 없는 자에게 공개되는 사례가 발견되고 있어 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다"라고 해설하고 있다.

고시 제6조제1항에 대해 "개인정보취급자 및 이용자의 비밀번호가 노출 또는 위·변조되지 않도록 일방향 함수(해쉬함수)를 이용하여 저장하여야 하며, 안전한 암호화 알고리즘은 CPU 및 메모리를 관련 장비의 발전에 따라 달라 질 수 있으나 일방향 해쉬함수의 경우 128비트 이상의 보안강도를 안전성을 권고한다"라고 해설하고 있다.

고시 제6조제3항에 대해 "신용카드번호, 계좌번호 등의 개인정보와 비밀번호, 바이오정보 등의 인증정보를 정보통신망 외부로 송·수신할 경우에는 해당 데이터를 임의의 사용자가 내용을 확인할 수 없도록 암호화 전송하여 노출 및 불법적인 접근을 차단하여야 한다"라고 해설하고 있다.

고시 제6조제4항에 대해 "고객의 개인정보를 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려 받아 저장할 때는 파일암호화 제품 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다"라고 해설하고 있다

나. 정보통신망법 제29조제1항은 "정보통신서비스 제공자등은 '제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우(제1호)' 등에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다."라고 규정하고 있다.

다. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자 등의 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 ① 개인정보처리자가 외부에서 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하여 추가적으로 안전한 인증수단을 적용하지 않았고, ② 개인정보에 대한 불법적인 접근을 차단하기 위한 비밀번호 작성 규칙을 수립하고 이를 적용·운영하지 않았고, ③ 취급중인 개인정보가 인터넷 홈페이지를 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터 및 모바일기기에 조치를 취하지 않았고, ④ 비밀번호는 복호화 되지 아니하도록 일방향 암호화(해쉬함수, 128비트 이상 보안강도)하여 저장하지 않았으며, ⑤ 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않았고, ⑥ 이용자의 이름, 전화번호, 주소 등 배송관련 개인정보가 담긴 엑셀파일(2,313건)을 개인용컴퓨터에 암호화하여 저장하지 않음으로써 정보통신망법 제28조제1항제2호(기술

적·관리적 보호조치 중 접근통제)·제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제2항제1호·제4호·제5호 및 제15조제4항제1호·제3호·제4호, 고시 제4조제4항·제8항·제9항 및 제6조제1항·제3항·제4항을 위반하였다.

나. 수집·이용목적을 달성한 개인정보를 파기하지 아니한 행위(법 제29조제1항)

정보통신서비스 제공자등은 정보통신망법 제29조제1항에 의해 개인정보의 수집·이용목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

그런데 피심인은 2010. 6. ~ 2017. 2.경까지 이동전화를 가입하는 과정에서 수집한 이용자의 가입신청서와 주민등록증 등 각종 신분증 사본 총 20,524건을 2017. 2. 7. 조사 당시까지 파기하지 아니하고 사무실 내 캐비넷, 박스와 PDF 파일형태로 개인정보처리시스템 내에 보유함으로서 정보통신망법 제29조(개인정보의 파기)제1항제1호를 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	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	§15②4호	개인정보취급자가 개인정보처리시스템에 접속 시, 숫자만으로 구성된 4자리의 비밀번호만으로도 접속이 가능하도록 하여 비밀번호의 생성 방법 및 변경 주기 등의 비밀번호 작성규칙을 수립하고 적용·운영하지 아니한 행위(고시§4⑧)
	접근 통제	§28①2호	§15②5호	로그인 하지 않아도 구글 등 검색엔진 URL주소 검색을 통해 열람권한 없는 자도 개인정보처리시스템에 접속하여 첨부파일(신분증, 가입신청서 등)을 다운로드 가능하도록 하여 취급중인 개인정보가 열람권한이 없는 자에게 공개 되거나 외부에 유출되지 않도록 조치를 취하지 아니한 행위(고시§4⑨)

	암호화	§28①4호	§15④1호	개인정보처리시스템 D/B에 비밀번호를 암호화 하지 아니하고 저장한 행위(고시§6①)
	암호화	§28①4호	§15④3호	정보통신망을 통해 비밀번호 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 하지 않은 행위(고시§6③)
	암호화	§28①4호	§15④4호	이용자의 배송관련 개인정보가 담긴 파일 2,313건을 개인용 컴퓨터에 암호화 하지 아니하고 저장한 행위(고시§6④)
	미파기	§29①1호		이용목적을 달성한 개인정보 20,524건('10.6.~'17.2. 경까지의 가입신청서와 주민등록증 등 각종 신분증 사본)을 파기하지 않고, 사무실 내 캐비넷과 박스 및 PDF 파일형태로 개인정보처리시스템에 보관

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 ① 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등 접근 통제장치의 설치·운영 및 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 이용자의 개인정보를 보호하기 위한 기술적·관리적 보호조치를 하여야 하고, ② 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

2. 시정명령 이행결과의 보고

피심인은 위반행위를 즉시 중지하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시결과를 포함한 재발 방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 과태료 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과태료는 같은 법 제76조제1항 제3호, 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 각각 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
o 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 행위에 대해서는 위반행위가 2개로 위반행위의 정도가 심하다고 판단되므로, 기준금액의 2분의 1인 500만원을 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 위반 건수가 많은 점 등을 고려하여 피심인에 대한 과태료를 감경하지 않는다.

다. 최종 과태료

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

< 과태료 산출내역 >

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

4. 수사기관 조사결과 이첩

피심인이 정보통신망법 제29조(개인정보의 파기)제1항제1호를 위반한 행위에 대하여는 같은 법 제73조제1의2호에 따라 2년 이하의 징역 또는 2천만원 이하의 벌금에 해당하여, 다음과 같이 처리한다.

피심인은 이동전화 개통 업무를 수행하면서 2012.2.21.부터 수집한 통신3사의 가입신청서 원본 또는 복사본 등 이용자 가입신청서 4,300여건을 사무실 내 캐비넷, 박스에 보관하는 등 방치하고, 2010.6.5.부터 수집한 개인정보처리시스템 내에

가입신청서 및 구비서류 등 개인정보 16,224건을 조사 당시인 2017.2.7.까지 파기하지 아니하였으며 신분증 스캐너 인식을 위해 이용자의 신분증 사본을 편집하여 출력하는 신분증 위조 정황이 발견되는 등 위반행위의 정도가 매우 심하다고 판단되므로 이번 사건에 대하여 시정명령을 부과하고, 조사결과는 수사기관에 이첩한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항, 제76조제1항제2호·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」 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 재판결과에 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)