방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 48 - 303호

안 건 명 통신사 영업점 등 24개사의 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2017. 12. 21.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하여서는 아니되며, ②외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰 인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, ③정보통신망을 통해 개인정보처리시스템에 불법적으로 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ④이용자의 계좌번호에 대해 안전한 암호알고리듬으로 암호화하여 저장하여야 하며, ⑤이용자의 개인정보 및 인증정보를 송·수신할 때

에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, ⑥이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화하여야 하며, ⑦동의를 받은 개인정보의 수집 및 이용목적을 달성한 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 : 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

피심인은 영리를 목적으로 이동통신서비스를 판매하는 등 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제25조에 따라 전기통신사업자로부터 개인정보 처리 위탁을 받은 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

방송통신위원회는 개인정보 취약분야인 통신사 영업점을 대상으로 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 기획조사(2017.5.17.) 하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

피심인은 아래와 같이 개인정보를 수집·보유하고 있다

< 개인정보 수집·보유 현황 >

구분	항목		수집기간	건수
컴퓨터	엑셀파일	주민등록번호		
		계좌번호 등 개인정보		
홈페이지	주민등록번호			
	이름,생년월일,주소,휴대전화번호,계좌번호 등			

가. 주민등록번호를 수집·이용한 행위

피심인은 기간동안 이동통신 및 인터넷서비스 등을 판매하면서 이용자의 주민등록번호 총 건을 수집하고, 업무용 컴퓨터(엑셀파일, 건) 및 홈페이지(건) 등에 저장한 사실이 있다.

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

(1) 피심인은 정보통신망을 통해 외부에서 개인정보처리시스템(http://)에 접속 시 단순히 아이디/패스워드만을 이용하여 접속하도록 한 사실이 있다.

(2) 피심인은 고객관리사설프로그램을 운영하면서 침입차단·탐지시스템 등 외부의 불법적인 접근을 차단하기 위한 접근 통제장치를 설치·운영하지 않은 사실이 있다.

(3) 피심인은 이용자의 개인정보(이름, 주소, 생년월일, 전화번호, 계좌번호 등)를 업무용 컴퓨터(엑셀파일, 건), 홈페이지(건) 등 총 건을 저장하면서 암호화하지 않은 사실이 있다.

(4) 피심인은 정보통신망을 통해 홈페이지의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화 하지 않은 사실이 있다.

다. 수집·이용 목적을 달성한 개인정보를 파기하지 아니한 행위

피심인은 수집·이용 목적을 달성한 개인정보 총 건을 파기하지 않은 사실이 있다.

라. 방송통신위원회는 2017. 7. 10. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2017. 7. 20. 의견을 제출하였다.

Ⅱ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제23조의2제1항은 "정보통신서비스 제공자는 '본인확인기관으로 지정받은 경우(제1호)', '법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우(제2호)', '영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우(제3호)'를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다."라고 규정하고 있다.

정보통신망법 제23조의2제1항제3호에 따라 고시한「영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자 고시」제1조는 "「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조의2 제1항 제3호에서 "영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자"라 함은 전기통신사업법 제38조 제1항 또는 제2항에 따라 기간통신사업자로부터 이동통신서비스를 도매 제공 받아 재판매하는 전기통신사업자를 말한다. 다만, 본문의 영업상 목적이란 휴대전화번호를 이용한 본인확인 서비스를 말한다."라고 규정하고 있다.

나. 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)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'를 하여야 한다."라고 규정하고 있다.

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

제15조제4항은 "개인정보가 안전하게 저장·전송될 수 있도록 '주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)', '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송수신하는 경우 보안서버 구축 등의 조치(제3호)', '그 밖에 암호화 기술을 이용한 보안조치'(제4호)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') 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."고 규정하고 있으며, 제5항은 "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.

제6조제2항은 "정보통신서비스 제공자등은 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다(제6호)."라고 규정하고 있으며, 제3항은 "이용자의 개인정보 및 인증정보를 송수신할 때는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나(제1호), 웹서버에 암호화 응용프로그램을 설치하여(제2호) 전송하는 정보를 암호화하여 송수신하는 기능을 갖추어야 한다."라고 규정하고 있으며, 제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

다. 정보통신망법 제29조제1항은 "정보통신서비스 제공자등은 '제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다."라고 규정하고 있으며, 제23조제1항 단서는 "다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다."라고 규정하고 있다.

라. 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. 주민등록번호를 수집·이용한 행위

피심인이 법적근거 없이 이용자의 주민등록번호를 수집·이용한 행위는 정보통신망법 제23조의2제1항(주민등록번호의 사용 제한)을 위반하였다.

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

피심인이 외부에서 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호 이외 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제1호, 고시 제4조제4항을 위반하였고,

피심인이 개인정보의 불법적인 접근을 차단하기 위한 침입차단 및 침입탐지 시스템을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제2호, 고시 제4조제5항을 위반하였고,

피심인이 이용자의 계좌번호 등 개인정보를 컴퓨터에 저장하면서 안전한 암호 알고리듬으로 암호화하지 않는 등의 행위는 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호 및 제4호, 고시 제6조제2항 및 제4항을 위반하였고,

피심인이 정보통신망을 통해 개인정보처리시스템의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등 암호화기술 등을 이용한 보안조치 등을 통해 암호화하지 않은 행위는 정보통신망법 제28조제1항제4호(기술적·관리적

보호조치 중 암호화), 시행령 제15조제4항제3호, 고시 제6조제3항을 위반하였다.

다. 수집·이용 목적을 달성한 개인정보를 파기하지 아니한 행위

피심인이 수집 목적을 달성한 이용자의 개인정보를 즉시 파기하지 않은 행위는 정보통신망법 제29조제1항(개인정보의 파기 중 목적을 달성한 경우)을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	주민등록번호	§23의2①		법적 근거없이 이용자의 주민등록번호를 수집·이용한 행위
	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)
	암호화	§28①4호	§15④2·4호	이용자의 이름, 전화번호, 계좌번호 등 개인정보를 암호화하지 않고 저장한 행위(고시§6②·④)
	암호화	§28①4호	§15④3호	이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위(고시§6③)
	미파기	§29①1호		이용목적을 달성한 개인정보를 파기하지 않고, 컴퓨터 등에 보관한 행위

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하여서는

아니되며, ②외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰 인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, ③정보통신망을 통해 개인정보처리시스템에 불법적으로 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ④이용자의 계좌번호에 대해 안전한 암호알고리듬으로 암호화하여 저장하여야 하며, ⑤이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, ⑥이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화하여야 하며, ⑦동의를 받은 개인정보의 수집 및 이용목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 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 제23조의2(주민등록번호의 사용 제한)제1항 및 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제2호·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 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(제67조에 따라 준용되는 경우를 포함한다.	법 제76조 제1항제2호	1,000	2,000	3,000
o 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 위반행위가 2개 이상인 경우이므로 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 정보통신망법 제23조의2제1항 및 제28조제1항 위반 행위에 대해서 특별히 해당사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§23의2①	1,000만원	없음	없음	**1,000만원**
§28①2·4호	1,000만원	500만원	없음	**1,500만원**
계				**2,500만원**

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제23조의2제1항 및 제28조제1항 위반에 대해 2,500만원의 과태료를 부과한다.

4. 수사기관 조사결과 이첩 등

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 인터넷 개통업무 등을 수행하면서 부터 컴퓨터 및 홈페이지에 수집한 이용자의 주민등록번호 등 개인정보 건을 조사 당시인 '17.5.17. 까지 파기하지 아니하고 보관하는 등 위반행위의 정도가 심하다고 판단되므로 이번 사건에 대하여 시정명령을 부과하고, 조사결과는 수사기관에 이첩한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제2호·제3호(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)