

방 송 통 신 위 원 회

심의 · 의결

안건번호 제2018 - 09 - 054호

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 이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ②이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화하여야 하며, ③동의를 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 : 5,000,000원

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 초고속인터넷서비스 판매 등과 관련된 개인정보 처리 위탁을 받은 사업자로 같은 법 제67조제2항에 따라 제28조 등의 규정이 준용되며, 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 피심인에 대한 이용자 민원(개인정보 무단열람)이 국민신문고에 접수(2017.2.1.)됨에 따라 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2017.7.13.)하였고, 다음과 같은 사실을 확인하였다.



2. 행위사실

가. 개인정보를 암호화하지 않고 저장한 행위

피심인은 업무용 컴퓨터에 고객의 개인정보(이름, 전화번호, 주민번호 앞자리, 통장계좌번호) 건을 엑셀파일(5개) 형태로 암호화 하지 않고 저장하였다.

<참고 1> 엑셀 파일에 저장된 초고속인터넷 가입자의 개인정보

	A	B	C	D	E	F	G	AF
5	유선	02월 01일	문	010-5850	87		기가콤팩트전환	광주 001-107-48
8	무선	02월 04일	이	010-7004	52	기변	76.8	농협 352-0045-4
14	유선	02월 06일	주	010-4064	66		기가콤팩트전환+기가와이파	농협 637046-52-0
22	유선	02월 13일		010-0838	74		기가콤팩트전환	농협 351-0048
24	무선	02월 16일	홍	010-5713	95	기변	76.8	농협 685-0208
32	무선	02월 20일	김	010-1767	65	기변	76.8	농협 601154-56-
35	유선	02월 20일	김	010-7624	61		기가콤팩트신규+otv10+otv10+기가	광주 080-121-08
40	유선	02월 23일	이	010-1222	77		기가콤팩트신규+otv12+기가와이	광주 736-121-53
43	무선	02월 26일	방	010-2083	95	MNP	76.8	농협 302-4662-20
44	무선	02월 27일	이	010-5674	65	기변	76.8	광주 083-122-0

나. 수집·이용 목적을 달성한 개인정보를 파기하지 아니한 행위

피심인은 부터 7월까지 가입완료 된 가입(변경)신청서 부와 엑셀 파일형태로 저장되어 있는 개인정보 건 등 총 건을 파기하지 않고 보관 하였다.

<참고 2> 매장 내 서랍에 보관중인 이용자의 가입신청서



다. 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 요청 하였으며, 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 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)’를 하여야 한다.”라고 규정하고 있다.

정보통신망법 시행령 제15조제4항은 “개인정보가 안전하게 저장·전송 될 수 있도록 ‘주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)’, ‘그 밖에 암호화 기술을 이용한 보안조치(제4호)’ 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’) 제6조제2항은 “정보통신서비스 제공자등은 계좌번호에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다(제6호).”라고 규정하고 있으며, 제4항은 “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 제6조제2항에 대해 개인정보 유·노출 시에 2차 피해가 발생할 확률이 높은 계좌번호 등에 대해서는 안전한 알고리즘(128비트 이상)으로 암호화하여 저장·관리해야 한다고 해설하고 있으며, 고시 제6조제4항에 대해 이용자의 개인정보를 업무용 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호알고리즘이 탑재된 암호화 소프트웨어 등을 활성화하거나 개인정보의 저장형태가 오피스 파일 형태일 때에는 해당 프로그램에서 제공하는 암호 설정 기능을 활용하고, MS Windows 등 운영체제에서 제공하는 암호화 기능을 활용하도록 해설하고 있다.

나. 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.

「정보통신망법 해설서」는 법 제29조제1항에 대해 개인정보 취급 위탁 시에도 위탁 업무에 따른 개인정보 이용 및 제공목적, 보유 및 이용기간 등을 정해 파기 사유가 발생하면 취급하고 있는 개인정보를 파기하도록 해야 한다고 해설하고 있다.

다. 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. 이용자의 계좌번호 등 개인정보를 암호화하지 않은 행위

피심인이 이용자의 계좌번호를 안전한 암호알고리즘으로 암호화하지 않고 저장하여 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호, 고시 제6조제2항을 위반하고, 이름·연락처·생년월일 등 이용자의 개인정보가 담긴 파일을 안전한 암호알고리즘으로 암호화하지 않고 업무용 컴퓨터에 저장하여 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제4호, 고시 제6조제4항을 위반하였다.

나. 수집·이용 목적을 달성한 개인정보를 파기하지 아니한 행위

피심인은 전기통신사업자로부터 처리 위탁받은 초고속인터넷서비스 판매 및 가입이 완료되어 수집·이용목적이 완료된 이용자 개인정보가 담긴 가입(변경)신청서류 및 엑셀파일 내의 개인정보를 파기하지 않고 보관함으로써 정보통신망법 제29조제1항제1호(개인정보의 파기 중 목적을 달성한 경우)을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	암호화	§28①4호	§15④2호	가입자의 계좌번호를 안전한 암호알고리즘으로 암호화하지 않고 저장한 행위(고시§6②)
	암호화	§28①4호	§15④4호	가입자의 개인정보를 암호화하지 않고 컴퓨터, 모바일 기기 및 보조저장매체에 저장한 행위(고시§6④)
	미파기	§29①1호		수집·이용 목적을 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 ① 이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ②이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화하여야 하며, ③동의를 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 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 위반행위에 대해서는 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

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 사업규모가 소기업*이며, 정보통신망법 제28조제1항에 따른 위반행위가 1개인 점을 감안하여 피심인에 대한 과태료를 기준금액에서 50%를 감경한다.

* 「중소기업기본법」 업종별 기준에 따라 평균 매출액 50억원 이하인 사업자(전자상거래, 방송통신업 등)

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28④호	1,000만원	없음	500만원	500만원
계				500만원

다. 최종 과태료

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

4. 벌 칙

피심인이 정보통신망법 제29조(개인정보의 파기)제1항제1호를 위반한 행위에 대하여는 같은 법 제73조제1의2호에 따라 2년 이하의 징역 또는 2천만원 이하의 벌금에 해당한다.

그러나 피심인은 ▲위반행위가 최초 적발된 점, ▲해당 사업자가 의견수렴 과정에서 개인정보를 모두 파기한 점 등을 감안하여 이번에 한해 시정명령만을 부과하고 향후 위반행위 적발 시 엄정하게 처리한다.

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.

위원장

이 효 성



부위원장

허 욱



위원

김 석 진



위원

표 철 수



위원

고 삼 석

