방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 13 - 072호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 , (사업자등록번호 :

대표이사

의 결 일 2017. 3. 15.

주 문

1. 피심인은 개인정보의 도난·유출을 방지하기 위하여 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 한다.

2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 10,000,000원

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 전자결제대행 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

구 분	2014년	2015년	2016년	평 균
매출액(단위 : 백만원)				
상시 종업원 수				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사대상

방송통신위원회는 국민 생활과 밀접한 결제대행서비스를 제공하는 정보통신서비스 제공자를 대상으로 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사(2016.8.16.~2016.8.17.) 하였고, 다음과 같은 사실을 확인하

였다.

2. 행위사실

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

1) 피심인은 결제정보관리시스템( )을 운영하면서 이용자들의 휴대전화번호, 성명, 생년월일, 통신사 정보 등을 직접 수집·관리하고 있고, 이 결제정보관리시스템을 토대로 가맹점에게 '가맹점 관리자 사이트(http://)'를 통해 접속하여 이용할 수 있는 결제정보조회 기능을 제공하고 있는데, 가맹점이 이용하고 있는 위 '가맹점 관리자 사이트'에서는 고객번호, 통신사명, 거래일시, 청구금액, 상품명, 결제승인번호, 휴대전화번호의 끝 네자리 등이 제공되고 있다.

2) 피심인은 개인정보취급자인 가맹점이 외부에서 정보통신망을 통해 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템(이하 '개인정보처리시스템'이라 한다)인 '가맹점 관리자 사이트'에 접속이 필요한 경우 단순히 아이디와 비밀번호만을 이용하여 접속이 가능하도록 하여, 불법적인 접근을 차단하기 위한 접근권한 부여기준을 수립·시행하지 않고, 안전한 인증수단(ex. 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기IP 인증 등)을 적용한 접근통제장치를 설치·운영하지 않았다.

나. 방송통신위원회는 2017. 1. 2. '개인정보보호 법규 위반사업자 시정조치(안) 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2017. 1. 12. 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 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)' 등의 조치를 하여야 한다."고 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) 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."고 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 필요하다고 해설하고 있다.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 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 개인정보취급자가 외부에서 피심인의 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단을 적용하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제4항을 위반하였다.

이에 대해 피심인은 가맹점에 제공하는 '가맹점 관리자 사이트'에서는 이용자의 휴대전화번호 중 중간의 네자리가 조회되지 않으므로(ex. 010-××××-1234), 이는 '개인정보처리시스템'에 해당되지 않는다고 주장한다.

그러나, 피심인은 결제정보관리시스템( )을 운영하면서 이용자들로부터 직접 휴대전화번호, 성명, 생년월일, 통신사 정보 등을 수집·관리하고 있으므로 위 결제정보관리시스템이 개인정보처리시스템임은 명백하다. 그리고, 이를 토대로 가맹점에 제공하는 '가맹점 관리자 사이트'에서도 휴대전화번호 끝자리 외에 고객번호, 통신사명, 거래일시, 청구금액, 상품명, 결제승인번호 등이 제공되고 있으며, 또한 가맹점이 자신의 고객들을 관리하기 위해 고객들의 완전한 휴대전화번호 등 이용자의 개인정보를 보유하고 있는 경우가 일반적이므로, 가맹점에 제공하는 '가맹점 관리자 사이트'에서 휴대전화번호 가운데 자리가 조회되지 않는다 하더라도, 가맹점으로서는 '가맹점 관리자 사이트'에서 제공하는 정보와 자신이 보유하고 있는 정보를 쉽게 결합하여 특정 개인을 식별할 수 있으며, 따라서 위 '가맹점 관리자 사이트'에서 제공하는 정보는 정보통신망법 제2조제1항제6호에 따른 개인정보에 해당한다고 할 것이다. 그러므로 위 '가맹점 관리자 사이트'는 '개인정보처리시스템'으로 보아야 한다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
(주)	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보의 도난·유출을 방지하기 위하여 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 한다.

2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

3. 과태료 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표 9] 및 「개인정보보호 의무위반자 과태

료 부과 등 처리지침」(이하 '처리지침')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 〉

위반사항	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 대해서 사업 규모, 위반의 동기 등을 고려하여 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 위반행위가 과실에 의한 것이라 볼 수 없고, 피심인의 사업규모 등을 고려하여 과태료를 감경하지 않는다.

< 과태료 산출내역 >

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

다. 최종 과태료

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

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항 및 제76조제1항제3호에 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 과태료를 납부하여야 한다.

위 원 장　　최 성 준 (인)

부위원장　　김 재 홍 (인)

위　　원　　김 석 진 (인)

※ 공무상 국외 출장('17.3.13.~3.16. EU, 벨기에)으로 전체위원회 불참

위　　원　　이 기 주 (인)

위　　원　　고 삼 석 (인)