방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 36 - 218호

안 건 명 개인정보 유출신고 사업자 등의 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2017. 10. 12.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 하며, 개인정보의 분실 도난·유출 사실을 안 때에는 지체 없이 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 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 제출하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 20,000,000원

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 온라인 쇼핑몰 웹사이트 를 운영하는 「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)				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

피심인이 운영 중인 웹사이트의 환불계좌 리스팅 페이지 42개 페이지에서 개인정보 420건이 웹상 노출 되었으며, 그 중 상세 페이지 항목(이름, 은행명, 계좌

번호) 25건이 권한 없는 타인에게 유출되었다는 피심인의 개인정보 유출신고(2017. 6. 15.)가 개인정보보호 포털(i-privacy.kr, KISA)에 접수됨에 따라, 방송통신위원회는 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사(2017. 6. 16.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

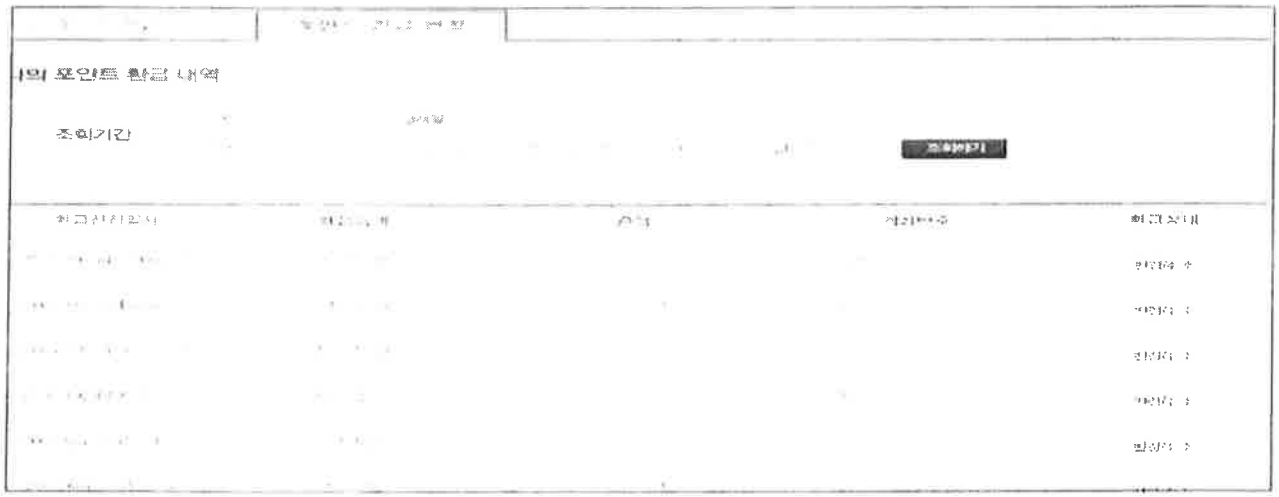
가. 개인정보 유출 통지·신고를 해태한 행위

피심인은 2017. 6. 14. 15:07부터 고객센터에 수건의 민원이 접수된 후 2017. 6. 14. 17:24 민원센터에서 담당부서로 민원내용을 공유한 사실로 볼 때, 최소한 2017. 6. 14. 17:24 이전에는 개인정보 유출사실을 인지하였음을 알 수 있으나, 2017. 6. 15. 18:25 한국인터넷진흥원에 이용자 개인정보 유출을 신고하였으며, 웹페이지 상에 개인정보가 노출되어 개인정보 유출 가능성이 있는 이용자 440명에게 2017. 6. 16. 15:33에 이메일을 통하여 관련 사실을 통보하였다.

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

피심인은 2017. 6. 14. 13시경 신규 메뉴(포인트 환급 현황) 버그 수정 과정에서 개발자 직원 실수로 유저 식별키 조건이 누락된 소스코드를 적용하여 이용자가 포인트 환급 현황 페이지 에 접속 시 타인의 개인정보 총 420건이 웹상 노출됨에 따라, 206명의 이용자가 타인의 개인정보(은행명, 계좌번호) 416건(중복제거)을 열람하고, 그 중 15명의 이용자가 상세 페이지(이름, 은행명, 계좌번호) 24건(중복제거)을 조회함으로써 인터넷 홈페이지를 통하여 열람권한 없는 자에게 타인의 개인정보가 공개되도록 한 사실이 있다

< 포인트 환급 현황 페이지 개인정보 노출 화면 >



다. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2017. 7. 4. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2017. 7. 14. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다, 2016. 9. 23. 이전에는 '유출' 대신 '누출'이라고 규정했었는데, 표현만 다를 뿐 같은 의미이다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다."라고 규정하고 있다.

정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 취급할

때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

나. 정보통신망법 시행령(2016. 5. 31. 대통령령 제27188호로 개정되기 전의 것. 이하 같다) 제14조의2제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다."라고,

제14조의2제2항은 "정보통신서비스 제공자등은 제1항에 따른 통지·신고를 하려는 경우 법 제27조의3제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다."라고,

제14조의2제3항은 "정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다."라고,

제14조의2제4항은 "천재지변이나 그 밖의 정당한 사유로 제3항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 제3항에 따른 홈페이지 게시를 갈음할 수 있다."라고,

제14조의2제5항은 "정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의

부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 방송통신위원회에 소명하여야 한다."라고 각 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'를 하여야 한다."라고 규정하고 있다.

다. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보 취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

라. 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. 개인정보 유출 통지·신고를 해태한 행위 (정보통신망법 제27조의3제1항)

피심인은 2017. 6. 14. 17:24 이전에는 개인정보 유출사실을 인지하였음을 알 수 있으나, 정당한 사유 없이 개인정보 유출사실을 안 때부터 24시간이 경과하여 방송통신위원회에 신고하고, 개인정보가 노출되어 개인정보 유출 가능성이 있는 이용자에게 이메일로 통지함으로써 정보통신망법 제27조의3제1항, 시행령 제14조의2제1항을 위반하였다.

피심인은 개인정보 노출사고 수습과 이용자에 대한 보상방안 마련에 예상보다 많은 시간이 소요되었다고 소명하고 있으나, 정보통신망법시행령 제14조의2제2항에 따라 개인정보의 유출 사실을 안 때부터 24시간 이내 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 이용자가 취할 수 있는 조치, 정보통신서비스 제공자등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처를 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인 즉시 통지·신고하여야 하므로 이유 없다 하겠다.

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

피심인은 운영 중인 홈페이지 이용자 포인트 환급 현황 페이지 개편 과정에서 홈페이지 취약점으로 인해 취급 중인 개인정보가 열람권한이 없는 자에게 공개되도록 함으로써, 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항제5호, 고시 제4조제9항을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	유출 신고	§27조의3①	§14조의2	개인정보 유출 사실을 안 때부터 24시간을 경과하여 이용자 통지·신고한 행위
	접근 통제	§28①2호	§15②5호	취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하지 아니한 행위(고시§4⑨)

Ⅳ. 시정조치 명령

1. 시정명령

가. 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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 제출하여야 한다.

3. 과태료 부과

피심인이 개인정보처리시스템에 기술적·관리적 보호조치를 하지 않은 행위 및 개인정보 유출 등 통지·신고를 지연한 행위에 대하여 정보통신망법 76조제1항 제2의3호, 제3호, 같은 법 시행령 제74조의 [별표 9] 및 「개인정보보호 의무위반자 과태료 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
ㅇ 법 제27조의3제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조 제1항제2의3호	1,000	2,000	3,000
ㅇ 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 제27조의3제1항 및 제28조제1항 위반 행위에 대해서 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 사업규모 등을 고려하여 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§27조의3①	1,000만원	없음	없음	**1,000만원**
§28①2호	1,000만원	없음	없음	**1,000만원**
계				**2,000만원**

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반에 대해 2,000만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제2호의3과 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 과태료를 납부하여야 한다.

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)