방 송 통 신 위 원 회
심의·의결

안건번호 제2020-28-125호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020년 5월 19일

주 문

1. 피심인은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 안전한 보안서버 구축 등의 조치를 통해 이를 암호화하여야 한다.

2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 금 액 : 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

1 (이하 '피심인'이라 한다.)는 영리를 목적으로 종합 온라인 쇼핑몰 ( ) 및 모바일 앱( )을 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 천원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

Ⅱ. 사실조사 결과

1. 조사 대상

2 방송통신위원회는 개인정보보호 포털에 유출신고한 사업자에 대하여 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2019.9.26., 9.30.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집 · 이용 현황

3 피심인은 온라인 쇼핑몰( ) 및 모바일 앱( )을 운영하면서 2019.9.25. 기준 건의 이용자 정보를 수집 · 보관하고 있다.

< 개인정보 수집 · 이용 현황 >

구분	항목	수집일	건수
회원 정보 (유효회원)	(필수) 성명, 생년월일, 휴대전화번호, 아이디, 비밀번호, 이메일 (선택) OK캐쉬백 멤버십 번호 등		건
(휴면회원)	최근 1년간 미사용자 탈퇴 처리		건
총 계			건

나. 개인정보 훼손 관련 사실관계

4 **(개인정보 훼손 경과 및 대응)**

5 - 2019.8.26. 10:37 민원인이 쇼핑몰 계정에 등록된 OK캐쉬백 포인트 소유주(어머니, 본인) 확인 요청

- 2019.8.26.~8.28. 민원인 본인 및 가족 명의의 OK캐쉬백 포인트 카드가 아닌 것으로 확인
- 2019.8.28.~9.9. 피심인, OK캐쉬백 운영사인 SK플래닛 간 적립 여부 및 오적립 여부에 대한 내부 확인 절차 진행
- 2019.9.19. 21:00 피심인은 전체 회원을 대상으로 의심 카드번호(11개)로 등록

된 계정 49,007개 확인

- 2019.9.20. 14:50 피심인은 의심카드 번호로 등록된 계정에서 멤버십 카드 제거
- 2019.9.20. 14:57 개인정보보호 포탈에 개인정보 유출 신고
- 2019.9.20. 18:00, 19:00 , OK캐쉬백이 무단 등록된 46,889명을 대상으로 이메일 및 문자메시지 통지

※ 통지 대상 중 2018.10.2.부터 2019.9.19.까지 비밀번호 변경 이력이 존재하는 2,118명은 통지 대상에서 제외

- 2019.9.23.~26. 온라인쇼핑몰 대상 취약점 점검 수행 및 이상여부 확인
- 2019.9.27. 15:20 온라인 쇼핑몰 홈페이지 내 계정 도용 사례 공지

6 **(훼손 규모 및 항목)** 이용자의 OK캐쉬백 정보 49,007건

7 **(훼손 경위)** 미상의 해커(이하 '이 사건의 해커'라 한다)는 알 수 없는 방법으로 2017.10.17.부터 2018.10.1.까지 피심인의 쇼핑몰 이용자 계정정보 49,007건에 대하여 OK캐쉬백* 포인트 적립번호를 이 사건의 해커 소유의 카드 11개의 번호로 등록함

* OK캐쉬백 : SK플래닛에서 운영하는 마일리지 시스템으로 구매금액의 0.05%를 포인트로 적립하고 가맹점에서 현금처럼 사용 가능

8 - 이 사건의 해커는 49,007건의 계정 중 2017.10.17.부터 2019.9.20.까지 주문 이력이 존재하는 14,361건의 계정에서 발생한 'OK캐쉬백 포인트' 4,009,170 포인트를 무단 적립함

※ SK플래닛을 통해 이 사건의 해커가 소유한 11개 카드 사용 내역을 확인 결과 3,000포인트(2017.11.30.)만 사용된 것으로 확인

3. 개인정보의 기술적·관리적 보호조치 등 사실관계

가. 개인정보를 전송하면서 암호화하지 않은 행위

9 피심인은 쇼핑몰에 로그인한 이용자 인증을 위해 http 패킷에 회원번호, 성별, 연령, 직업, , 로그인 정보, 로그인 정보, 이름(URL 인코딩)

등의 이용자의 개인정보 및 인증정보를 송·수신할 때 전송되는 구간을 암호화하지 않고 평문으로 전송한 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

10 방송통신위원회는 2020. 2. 25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2020. 3. 13. 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.

11 정보통신망법 시행령 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치(제3호)'와 '그밖의 암호화기술을 이용한 보안조치(4호)'를 하여야 한다."라고 규정하고 있다.

12 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 고시 제6조제3항은 "이용자의 개인정보 및 인증정보를 송수신할 때는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나(제1호), 웹서버에 암호화 응용프로그램을 설치하여(제2호) 전송하는 정

보를 암호화하여 송수신하는 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."라고 규정하고 있다.

13 '고시 해설서'는 고시 제6조제3항에 대해 정보통신서비스 제공자등은 이용자의 성명, 연락처 등의 개인정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 하며, SSL(Secure Sockets Layer)인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화하여 전송하는 방식이며, 응용프로그램을 이용한 보안서버는 웹서버에 접속하여 보안 프로그램을 설치하여 이를 통해 개인정보를 암호화 전송하는 방식이라고 해설하고 있다.

나. 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. 개인정보를 전송하면서 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**하지 않은 행위**

14 피심인이 쇼핑몰에 로그인한 이용자의 개인정보(회원번호, 성별, 연령, 직업, 대표점포, 마트 로그인 정보, SSO 로그인 정보, 이름(URL 인코딩)) 및 인증정보를 정보통신망을 통해 송·수신할 때 암호화하지 아니한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제3호, 고시 제6조제3항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단시스템을 설치·운영을 소홀히 한 행위(고시§4⑤)
	암호화	§28①4호	§15④3호	이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위(고시§6③)

Ⅳ. 시정조치 명령

1. 시정명령

15 피심인은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 안전한 보안서버 구축 등의 조치를 통해 이를 암호화하여야 한다.

2. 시정명령 이행결과의 보고

16 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

Ⅴ. 과태료 부과

17 피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

18 정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 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)** 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

19 그러나 피심인은 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

20 이에 따라 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 500만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①4호	1,000만원	없음	500만원	**500만원**
계				**500만원**

다. 최종 과태료

21 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 5,000,000원의 과태료를 부과한다.

Ⅵ. 결론

22 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 따라 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 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.

이에 주문과 같이 의결한다.

2020년 5월 19일

위 원 장 한 상 혁 (인)

부위원장 표 철 수 (인)

위 원 허 욱 (인)

위 원 김 창 룡 (인)

위 원 안 형 환 (인)