방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 33 - 159호

안 건 명 개인정보 및 위치정보 보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020. 6. 4.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

가. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

나. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스

템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

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

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

마. 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 쇼핑몰 서비스( )를 운영하는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 매출액 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

2. 방송통신위원회는 온라인 개인정보보호 포털(i-privacy.kr)에 개인정보 유출을 신고한 피심인에 대하여 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2019. 3. 13.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 오픈마켓 서비스인 을 운영하면서 2019. 3. 12.현재 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
이용자정보 (유효회원)	성명, 성별, 생년월일, 이동전화번호, 이메일 주소 등		건
(휴면회원)	상 동		건
합 계			건

나. 개인정보 유출경위

1) 개인정보 유출 경과 및 대응

가) 2018. 8. 개인정보 유출 관련

- 2018. 8. 22. 기자의 연락을 받고 계정이 중국에서 거래되고 있다는 사실을 인지
- 2018. 8. 22. 17시경 방송통신위원회의 "언론보도 관련 사실관계 확인 요청" 메일을 수신하고 bo****아이디가 해외 IP에서 접속한 사실을 확인하는 과정에서 중국 IP(221.X.X.X)에서 해당 ID로 부정 접속한 사실을 확인

나) 2019. 1. 개인정보 유출 관련

- 2019.1.9. 10:00 기프트카드 이벤트 오픈
- 2019.1.9. 12:10 기프트카드를 구매한 경우 배송정보를 조회하고 LMS 재발송을 요청하는 페이지에서 다른 이용자의 개인정보(이름, 전화번호, 배송지 주소)가 조회된다는 사실을 인지
- 2019.1.9. 14시경 해당 오류가 발생한 원인을 수정
- 2019.1.9. 19:29 기프트카드 이벤트 구매 폭주로 인해 다른 이용자에게 개인정보가 노출되었다고 개인정보보호 포털(i-privacy.kr)에 신고

2) 개인정보 유출 규모

가) 2018. 8. 개인정보 유출 관련

4. 신원 미상의 해커(이하 '이 사건 해커'라 한다)는 피심인이 온라인 쇼핑몰 오

픈마켓 서비스를 운영하면서 수집한 이용자의 계정정보(아이디, 비밀번호)를 알수 없는 방법으로 취득하여 부정 접속하였으나, 개인정보를 열람·유출하였는지 여부는 확인할 수 없었다.

나) 2019. 1. 개인정보 유출 관련

5. 피심인이 기프트카드 주문관련 페이지에 주문정보와 토큰정보의 일치 여부를 확인하는 소스코드를 누락하여 2019. 1. 9. 12:10 경 이용자가 기프트카드를 구매한 경우 배송정보를 조회하고 LMS 재발송을 요청하는 페이지에서 다른 이용자(2명)의 개인정보가 조회되었다. 조회된 개인정보 항목은 이름, 전화번호, 배송지 주소 등이다.

3) 개인정보 유출 경로

가) 2018. 8. 개인정보 유출 관련

6. 피심인은 2018. 8. 22. 기자의 연락을 받고 계정이 중국에서 거래되고 있다는 사실을 인지하였고, bo****아이디가 해외 IP에서 접속한 사실을 확인하는 과정에서 중국 IP에서 해당 ID가 부정 접속한 사실을 확인하였다.

7. 피심인이 보관하고 있는 웹로그 등을 분석한 결과,

① 해당 중국IP(221.209.)에서 2018. 8. 19.부터 2018. 8. 25.까지 건 로그인 시도가 있었음을 확인하였다.

② 로그인을 시도한 IP의 로그인 성공·실패 건수를 확인한 결과, 건의 로그인 시도 중 건(ID: 개)이 로그인에 성공하였고, 건이 로그인에 실패한 것을 확인하였다.

③ 부정 로그인에 성공한 건(ID: 개)이 피심인의 홈페이지의 어떤 페이지에 접속하였는지에 대한 로그는 확인되지 않았다.

나) 2019. 1. 개인정보 유출 관련

8. 피심인은 2014년경 '기프트카드 주문 관련 페이지'를 개발하는 과정에서 주문번호와 토큰정보의 일치 여부를 확인하는 소스코드를 누락하였고, 해당 페이지를 수정작업 없이 유지하고 있다가 2019. 1. 9. 진행한 '기프트카드 이벤트'에 해당 페이지의 이용자 폭주로 이용자 2명의 개인정보가 타인에게 노출되었다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템의 접근통제를 소홀히 한 행위(정보통신망법 제28조 제1항제2호)

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치 · 운영을 소홀히 한 행위

9. 피심인은 무작위로 아이디, 비밀번호를 입력하여 로그인을 시도하는 사전 대입공격 등을 탐지·차단하기 위하여 자체적으로 '부정 로그인 탐지시스템'을 구축하여 운영하고 있었으나, 중국IP(221.209.)가 2018. 8. 19.부터 2018. 8. 25.까지 시도한 부정 로그인을 탐지·차단하지 못한 사실이 있다.

2) 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 소홀히 한 행위

10. 피심인은 2014년경 '기프트카드 주문 관련 페이지'를 개발하는 과정에서 주

문번호와 토큰정보의 일치 여부를 확인하는 소스코드를 누락하였지만 정상적으로 매칭하여 주문자 정보를 이상 없이 제공해 왔으나, 2019. 1. 9. 10시부터 진행한 '기프트카드 이벤트' 구매 폭주로 인해 다른 이용자에게 서비스 이용자 2명의 개인정보가 2019. 1. 9. 13시경 노출된 것을 인지하고 2019. 1. 9. 14시경 해당 오류가 발생한 원인을 수정한 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

11. 방송통신위원회는 2019. 4. 18. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 5. 16. 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)' 하여야 한다."라고 규정하고 있다.

12. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

13. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통

신위원회 고시 제2015-3호, 이하 '고시') 제4조제5항은 "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 있고, 제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

14. '고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하며, 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며 신규 위협 대응 및 정책의 관리를 위하여 지속적인 업데이트 적용 및 운영·관리, 이상 행위 대응 등의 방법을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있고,

15. 고시 제4조제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서

의 개인정보 유·노출 방지 조치를 하여야 하며, 인터넷 홈페이지 운영·관리 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하여야 한다고 해설하고 있다.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 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. 개인정보처리시스템의 접근통제를 소홀히 한 행위(정보통신망법 제28조제1항)

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위

16. 피심인이 신규 위협 대응, 정책 설정 운영, 이상 행위 대응, 로그 분석 등의 방법을 활용하여 접근 제한 및 유출 탐지 기능이 충족되도록 침입탐지시스템 등을 체계적으로 운영·관리하지 않아 중국IP(221.209.)에서 2018. 8. 19. 부터 2018. 8. 25.까지 개의 부정 로그인한 행위를 탐지하지 못하는 등 침입차단 및 탐지시스템을 소홀히 설치·운영한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항, 고시 제4조제5항을 위반한 것이다.

2) 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 소홀히 한 행위

17. 피심인이 2014년 경 최초 개발한 후 별도의 수정 및 검증작업 없이 기프트

카드 이벤트를 하는 과정에서 주문정보와 토큰정보의 일치 여부를 확인하는 소스코드를 누락하여 열람권한이 없는 자에게 개인정보가 공개되게 한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위(고시 §4⑤)
	접근 통제	§28①2호	§15②	열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 소홀히 한 행위(고시 §4⑨)

Ⅳ. 시정조치 명령

1. 시정명령

18. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다. 1)정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것 2)취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

2. 시정명령 이행결과의 보고

19. 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

20. 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

21. 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.

22. 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.

23. 이에 따라 조사 과정 중 법규 위반 행위를 중지하고 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
§28①2호	1,000만원	없음	500만원	**500만원**
계				**500만원**

다. 최종 과태료

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

Ⅵ. 결론

25. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

26. 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.

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

28. 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 6월 4일

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)