방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 38 - 172호

안 건 명 개인정보 유출신고 사업자의 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020. 6. 24.

주 문

1. 피심인은 개인정보의 분실 · 도난 · 유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지 · 신고해서는 아니 된다.

2. 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. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권

한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

나. 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화할 것

3. 피심인은 제1항부터 제2항까지의 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.

4. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 21,000,000원

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 화장품 판매 사이트 를 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 : 백만원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				
관련 매출				
관련없는 매출				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성하였으며 해당 사이트는 2017 부터 운영

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. 11. 14.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 화장품 판매를 위한 사이트 를 운영하면서, 2019. 11. 14. 현재 아래와 같이 이용자의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
이용자 정보 (유효회원)	이름, 로그인ID, 비밀번호, 성별, 이메일, 휴대전화번호, 생년월일, 주문기록 등 서비스 이용기록, 가입경로		건
(휴면회원)			건
합 계			건

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019. 11. 10. 04:38 피심인의 이용자는 사이트 1:1게시판을 통해 2,507명의 개인정보가 담긴 파일(회원목록다운로드 .xlsx)이 구글 검색을 통해 노출된다는 게시글을 남김
- 2019. 11. 10. 13:30 피심인은 이용자의 개인정보파일 구글 노출 관련 게시글을 열람하고 유출 사실을 인지함
- 2019. 11. 10. 14:30 피심인은 개인정보처리시스템 내 개인정보파일(회원목록다운로드 .xlsx) 삭제 및 구글에 검색되지 않게 조치함
- 2019. 11. 12. 19:38 피심인은 한국인터넷진흥원에 개인정보 유출 신고함
- 2019. 11. 13. 15:11 피심인은 이용자 개별통지(이메일) 및 홈페이지 공지

2) 개인정보 유출 규모

4. 피심인의 이용자 2,507명의 개인정보가 담긴 엑셀파일이 구글 검색엔진에 노출되었다.

< 피심인의 개인정보 노출현황 >

구 분	노 출 항 목	건 수
회원정보	아이디, 이름, 휴대전화번호, 성별, 이메일, 생년월일	2,507건

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보의 분실 · 도난 · 유출 사실을 지연 통지·신고한 행위

5. 피심인은 2,507명의 이용자 개인정보가 담긴 개인정보파일(회원목록다운로드.xlsx)이 구글에 노출 되었다는 게시글(2019. 11. 10. 04:38)을 확인(2019. 11. 10. 13:30)하고 인지하였으나, 24시간을 경과하여 유출신고(2019. 11. 12. 19:38) 및 통지(2019. 11. 13. 15:11)를 실시한 사실이 있다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

6. 피심인은 개인정보처리시스템 내 저장된 개인정보파일을 구글 등 검색엔진에 검색 및 다운로드 되지 않도록 조치를 취하지 않는 등의 원인으로, 열람권한이 없는 자에게 노출되게 한 사실이 있다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

7. 피심인은 이용자 2,507명의 개인정보가 담긴 개인정보파일을 개인정보처리시스템에 암호화하지 않고 평문으로 저장한 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

8. 방송통신위원회는 2020. 5. 1. '개인정보보호 법규 위반사업자 시정조치(안)사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2020. 5. 18. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다."라고 규정하고 있다.

9. 정보통신망법 시행령 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."고 규정하고 있으며, 제2항은 "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 규정하고 있다.

10. '정보통신망법 해설서'는 정보통신망법 제27조의3제1항의 '지체 없이'에 대해서 정보통신망법에 별도로 규정된 정의는 없으나, 관련 판례에서는 '합리적인 이유 및 근거가 없는 한 즉시'로 해석하고 있다.

나. 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)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용

한 보안조치(제4호)' 하여야 한다."라고 규정하고 있다.

11. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'를 하여야 한다."라고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '그 밖에 암호화기술을 이용한 보안조치(제4호)'를 하여야 한다."라고 규정하고 있다.

12. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)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 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

13. 고시 제6조제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

14. '고시 해설서'는 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 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 한다고 해설하고 있다.

15. 고시 제6조제4항에 대해 이용자의 개인정보를 업무용 컴퓨터, 모바일 기기

및 보조저장매체 등에 저장할 때에는 안전한 암호알고리듬이 탑재된 암호화 소프트웨어 등을 활용하거나 개인정보의 저장형태가 오피스 파일 형태일 때에는 해당 프로그램에서 제공하는 암호 설정 기능을 활용하고, MS Windows 등 운영체제에서 제공하는 암호화 기능을 활용하도록 해설하고 있다.

다. 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. 개인정보의 분실·도난·유출 사실을 지연 통지·신고{정보통신망법 제27조의3(개인정보 유출등의 통지·신고)}**한 행위**

16. 피심인이 2,507명의 이용자 개인정보가 담긴 개인정보파일(회원목록다운로드 .xlsx)이 구글에 노출 되었다는 게시글(2019. 11. 10. 04:38)을 확인(2019. 11. 10. 13:30)하고 인지하였으나, 24시간을 경과하여 유출신고(2019. 11. 12. 19:38) 및 통지(2019. 11. 13. 15:11)한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

17. 피심인이 개인정보처리시스템( )에 저장된 개인정보파일을 구글 등 검색엔진에 검색 및 다운로드 되지 않도록 조치를 취하지 않아, 2019. 11. 10. 01:42 ~ 2019. 11. 10. 14:02 기간 동안 열람권한이 없는 자(IP 66.249. - 미국 등 7개)에게 개인정보파일(회원목록다운로드 .xlsx)이 노출되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법

시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

다. 개인정보의 암호화기술 등을 이용한 보안조치{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

18. 피심인이 이용자 2,507명의 개인정보가 담긴 개인정보파일(회원목록다운로드 .xlsx)을 개인정보처리시스템 내 저장장치에 암호화하지 않고 평문으로 보관한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제4항제4호, 고시 제6조제4항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	지연 신고 통지	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
	암호화	§28①4호	§15④4호	개인정보를 컴퓨터 등에 저장할 때 암호화하지 않은 행위(고시§6④)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된

다.

나. 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)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)이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화할 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 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제2호의3·제3호, 같은 법 시행령 제74조의 [별표 9] 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 피심

인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 각 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
하. 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 제1항제2호의3	1,000	2,000	3,000
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 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

22. 이에 따라 피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 경우에 해당하므로 기준금액의 30%인 300만원을 각 가중한다.

< 과태료 부과지침 [별표 2] '과태료의 가중기준' >

기준	가중사유	가중비율
위반의 정도	가. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 50% 이내

	나. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 하목 가. 정보통신망법 제27조의3제1항을 위반하여 이용자에게 통지하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지한 경우 나. 정보통신망법 제27조의3제1항을 위반하여 방송통신위원회 또는 한국인터넷진흥원에 신고하지 아니하거나 정당한 사유 없이 24시간을 경과하여 신고한 경우	
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 너목 가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부 관리계획의 수립·시행을 하지 않은 경우 나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우 다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우 라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우 마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치를 하지 않은 경우 바. 정보통신망법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하지 않은 경우	

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 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

23. 이에 따라 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 정보통신망법 제28조제1항 위반 과태료에 대해 기준금액의 50%인 500만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§27의3①	1,000만원	300만원	없음	**1,300만원**
§28①2·4호	1,000만원	300만원	500만원	**800만원**
계				**2,100만원**

다. 최종 과태료

24. 이에 따라 피심인의 정보통신망법 제27조의3제1항, 제28조제1항 위반행위에 대해 21,000,000원의 과태료를 부과한다.

Ⅵ. 결론

25. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항(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 효

력을 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 24일

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)