

방 송 통 신 위 원 회

심 의 · 의 결

안건번호 제2020-23-107호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020년 4월 29일

주 문

1. 피심인은 정보통신서비스 제공자로서 제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁함에 있어서 개인정보 처리위탁을 받는 자와 개인정보 처리위탁을 하는 업무의 내용을 모두 이용자에게 알리고 동의를 받거나, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우에는 개인정보 처리위탁을 받는 자 및 개인정보 처리위탁을 하는 업무 내용을 개인정보처리방침에 정하여 이를 이용자가 언제든지 쉽게 확인할 수 있도록 공개하거나 전자우편·서면·모사전송·전화 또는 이와 유사한 방법을 통해 이용자에게 알려야 한다.
2. 피심인은 정보통신서비스 제공자로서 제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁할 때에는 문서에 의하여야 한다.
3. 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.

4. 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. 개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여할 것

나. 개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관할 것

다. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것

라. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독할 것

5. 피심인은 제1항부터 제4항까지의 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.

6. 피심인에 대하여 다음과 같이 과태료를 부과한다.



가. 금 액 : 25,500,000원

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)은 영리를 목적으로 온라인 화장품 쇼핑몰 ()을 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신 서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수('19.2.20.기준)

< 피심인의 최근 3년간 매출액 현황 >

(단위 : 천원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				
관련 매출				
관련 없는 매출**				

※ 자료 출처 : 이 제출한 재무제표 등 회계자료를 토대로 작성

* 사업개시 후 3년이 되지 않아, 정보통신망법 시행령 제69조의2제1항 단서에 따라 사업개시 후 '18년 말까지의 매출액을 연평균 매출액으로 환산

** 매출 등은 관련 없는 매출로 분류

II. 사실조사 결과

1. 조사 대상

- 2 방송통신위원회는 개인정보보호 포털(i-privacy.kr, KISA)에 유출신고한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2019. 2. 19. ~ 2. 20.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

- 3 피심인은 인터넷 화장품 쇼핑몰()을 운영하면서 2019.2.19. 기준 건의 이용자 정보를 수집·보관하고 있다.

< 개인정보 수집·이용 현황 >

구분	항목	수집일	건수
회원 정보 (유효회원)	아이디, 비밀번호, 휴대전화번호, 나이, 이메일, 주소	~ '19.2.19.	건
(휴면회원)	상동	~ '18.2.18.	건
총 계			건

나. 유출 규모 및 항목

- 4 피심인이 온라인 화장품 판매 홈페이지()를 운영하면서 수집한 회원정보 약 10,000건이 유출되었다. 유출된 개인정보 항목은 아이디, 이름, 휴대전화번호, 이메일 등 4개 항목이다.



< 피심인의 개인정보 유출 현황 >

구분	유 출 항 목	건 수
홈페이지 회원	아이디, 이름, 휴대전화번호, 이메일 등	약 10,000건

다. 유출 경위

- 5 미상의 해커(IP:222.117.171. , 이하 ‘이 사건의 해커’라 한다)는 알 수 없는 방법으로 관리자 계정을 취득한 후, 2018. 12. 7. 17:09 관리자 페이지에 접속하여 2018. 12. 7. 17:13 () 회원정보를 엑셀파일로 다운로드하였다.

< 이 사건의 해커가 보낸 협박메일 내용 >

라. 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
2018.12.7.	17:13	이 사건의 해커는 회원정보 엑셀파일을 다운로드 함
	17:14	이 사건의 해커는 전체 유효회원 대상(7,553명)으로 “ 회원 개인정보 유출안내” 제목의 공지 메일을 발송하였고 피심인은 개인정보 유출사실을 인지함
2018.12.9.	16:44	이 사건의 해커는 ‘ 관계자분들 보세요’라는 제목의 협박 메일을 발송
2018.12.11.	15:36	개인정보보호 포털(i-privacy.kr)에 개인정보 유출 신고함
	16:00	사이버수사대 수사 의뢰, 개인정보 유출사실을 홈페이지에 공지하고 카카오톡을 이용하여 이용자 대상 통지함

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보의 처리위탁 내용을 이용자에게 공개하지 않은 행위{정보통신망법 제25조(개인정보의 처리위탁) 중 개인정보 처리위탁의 공개}

6 피심인은 에 쇼핑몰 개인정보 처리 업무(저장, 보유 등)를 위탁하고 있으나 이용자에게 이에 대해 동의를 받은바 없고 개인정보처리방침에도 공개하지 않은 사실이 있다.

< 피심인의 개인정보처리방침-개인정보처리 위탁 부분 >

나. 개인정보의 처리위탁 시 문서에 의하지 않은 행위{정보통신망법 제25조(개인정보의 처리위탁) 중 문서를 통한 처리위탁}

7 피심인은 에 쇼핑몰 개인정보 처리 업무(저장, 보유 등)를 위탁하면서 별도의 개인정보 처리 위탁계약서 등 문서를 통해 위탁한 사실이 없다.

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

8 피심인은 쇼핑몰을 운영하면서 2018. 12. 7. 미상의 해커가 발



송한 “ 회원 개인정보 유출안내” 제목의 이메일을 받고서 개인정보 유출사실을 인지하였으나 3일이 경과한 2018. 12. 11. 개인정보보호 포털 (i-privacy.kr)에 신고하고 이용자에게 통지한 사실이 있다.

라. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}

9 (접근권한 최소 부여) 피심인은 쇼핑몰을 운영하면서 관리자 페이지()에 총 5개(관리자, CS팀, 물류팀, MD파트, 디자인팀)의 접속계정을 운영하고 있었으나 개인정보취급자별 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화하여 접근권한을 부여하지 않은 사실이 있다.

10 (접근권한 기록 보관) 피심인은 개인정보를 처리하는 관리자 페이지 ()에 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 보관해야하나, 그 이력을 보관하지 않은 사실이 있다.

11 (안전한 인증수단) 피심인은 쇼핑몰 관리자페이지 접속 시 아이디와 비밀번호 이외에 추가적인 안전한 인증수단을 적용하지 않은 사실이 있다.

< 피심인의 로그인 보안 설정-2차인증 및 중복로그인 제한 기능을 비활성화 >



마. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위
{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}

12 피심인은 개인정보처리시스템의 개인정보취급자에 대한 접속기록을 6개월간 보관하고 있었으나, 그 기록을 월 1회 이상 정기적으로 확인·감독하지 않은 사실이 있다.

< 이 사건의 해커가 회원정보를 엑셀로 다운로드한 접속기록 >



바. 처분의 사전통지 및 의견 수렴

13 방송통신위원회는 2019. 4. 18. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 4. 23. 의견을 제출하였다.

III. 위법성 판단

1. 관련법 규정



가. 정보통신망법 제25조제2항은 “정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.”라고 규정하고 있고, 제6항은 “정보통신서비스 제공자등이 수탁자에게 개인정보 처리위탁을 할 때에는 문서에 의하여야 한다.”라고 규정하고 있다.

14 정보통신망법 시행령 제10조는 “법 제25조제2항 전단에서 ‘대통령령으로 정하는 방법’이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다.”라고 규정하고 있다.

15 ‘정보통신망법 해설서’는 “법 제25조제2항에 대해 다만, 정보통신서비스 제공에 관한 계약의 이행을 위하여 필요한 경우에는 당해 위탁업무의 내용 및 수탁자를 이용자가 언제든지 확인할 수 있도록 개인정보처리방침에 공개하거나, 전자우편·서면·모사전송·전화 또는 이와 유사한 방법(시행령 제10조)으로 이용자에게 통지하는 것으로 이용자에게 동의를 얻어야 하는 의무를 대신할 수 있습니다. 즉, 이용자에게 서비스를 제공하기 위해 어쩔 수 없이 발생하는 위탁에 대해서는 ①누구에게 ②왜 주는지에 대해서 이용자가 알도록 조치하면 되고, 별도로 동의를 받을 필요는 없습니다.”라고 설명하고 있다.

나. 정보통신망법 제27조의3제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 ‘유출등이 된 개인정보 항목(제1호)’, ‘유출등이 발생한 시점(제2호)’, ‘이용자가 취할 수 있는 조치(제3호)’, ‘정보통신서비스 제공자등의 대응 조치(제4호)’, ‘이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)’의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.”라고



규정하고 있다.

16 정보통신망법 시행령 제14조의2제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 이메일·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.”라고 규정하고 있으며, 제2항은 “정보통신서비스 제공자등은 제1항에 따른 통지·신고 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.

17 ‘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.

다. 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)’, ‘접속기록의 위조·변조 방지를 위한 조치(제3호)’를 하여야 한다.”라고 규정하고 있다.

18 정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제15조제3항은 “정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역



등의 저장 및 이의 확인·감독(제1호) 등의 조치를 하여야 한다.”라고 규정하고 있다.

19 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 ‘고시’) 고시 제4조제1항은 “정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.”라고 규정하고 있고, 제3항은 “정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.”라고 규정하고 있으며, 제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”고 규정하고 있다.

20 ‘고시 해설서’는 고시 제4조제1항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여하여야 하며 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요가 있으며, 개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 한다고 해설하고 있고, 제4조제3항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 5년간 보관하여야 하며, 관리대장 등에는 신청자 정보, 신청 및 적용 일시, 승인자 및 발급자 정보, 신청 및 발급사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하여야 한다고 해설하고 있다

21 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호

번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있다.

22 고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다고 해설하고 있다.

라. 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. 개인정보의 처리위탁 내용을 이용자에게 공개하지 않은 행위{정보통신망법 제25조(개인정보의 처리위탁) 중 개인정보 처리위탁의 공개}

23 피심인이 쇼핑몰 개인정보 처리업무(저장, 보유 등)를 ‘회사에 개인정보처리위탁하면서 개인정보처리방침에 개인정보 처리위탁 업무내용 및 수탁자등을 공개하거나 전자우편·서면·모사전송·전화 등을 통해 이용자에게 알리지 않은 행위’는 정보통신망법 제25조제2항을 위반한 것이다.

나. 개인정보의 처리위탁 시 문서에 의하지 않은 행위{정보통신망법 제25조(개인정보의 처리위탁) 중 문서를 통한 처리위탁}

24 피심인은 ‘에 쇼핑몰 개인정보 처리 업무(저장, 보유



등)를 위탁하면서 별도의 개인정보 처리 위탁계약서 등 문서에 의해 처리위탁하지 않은 행위는 정보통신망법 제25조제6항을 위반한 것이다.

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

25 피심인이 개인정보 유출사실을 2017.12.7. 인지 후 3일이 경과한 2018.12.11.에 개인정보보호 포털(i-privacy.kr)에 신고하고 이용자에게 통지한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

라. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}

26 **(접근권한 최소 부여)** 피심인이 쇼핑몰을 운영하면서 개인정보취급자별 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 접근권한을 부여하지 않고, 팀별로 총 5개(관리자, CS팀, 물류팀, MD파트, 디자인팀)의 접속계정을 개인정보취급자가 공용 사용한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제1항을 위반한 것이다.

27 **(접근권한 기록보관)** 피심인이 관리자 페이지에 대한 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년 이상 보관하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

28 **(안전한 인증수단)** 피심인이 개인정보취급자가 외부에서 피심인의 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항제2호,



같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

마. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위
{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}

29 피심인이 개인정보처리시스템에 접속한 접속기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	처리위탁 공개	§25②3호	§10	개인정보 처리 위탁사를 개인정보 처리방침에 공개하지 않음
	문서에 의한 처리위탁	§25⑥	-	개인정보 처리 위탁 시 문서에 의하지 않은 행위
	지연 신고	§27의3①	§14의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근 통제	§28①2호	§15②1호	개인정보처리시스템에 대한 접근권한을 부여할 때 필요한 범위에서 구체적으로 차등화 하여 부여하지 아니한 행위(고시§4①)
	접근 통제	§28①2호	§15②1호	개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 확인·감독하지 않은 행위(고시§5①)

IV. 시정조치 명령



1. 시정명령

가. 피심인은 정보통신서비스 제공자로서 제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁함에 있어서 개인정보 처리위탁을 받는 자와 개인정보 처리위탁을 하는 업무의 내용을 모두 이용자에게 알리고 동의를 받거나, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우에는 개인정보 처리위탁을 받는 자 및 개인정보 처리위탁을 하는 업무 내용을 개인정보처리방침에 정하여 이를 이용자가 언제든지 쉽게 확인할 수 있도록 공개하거나 전자우편·서면·모사전송·전화 또는 이와 유사한 방법을 통해 이용자에게 알려야 한다.

나. 피심인은 정보통신서비스 제공자로서 제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁할 때에는 문서에 의하여야 한다.

다. 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.

라. 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)개인정보처리시스템에 열람, 수정, 다운로드 등 본인 이외의 개인정보에 대한 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여할 것 2)개인정보 취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최



소 5년간 보관할 것 3)개인정보취급자가 정보통신망을 통해 외부에서 개인정보 처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것 3)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독할 것

2. 시정명령 이행결과의 보고

30 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

31 피심인의 정보통신망법 제25조(개인정보의 처리위탁)제1항·제2항, 제27조의 3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제2호의3·제3호, 제76조제2항제1호, 제76조제3항제2호의5 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

32 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 과태료를 각 적용한다.

〈 위반 횟수별 과태료 금액 〉

1회	2회	3회	4회	5회	6회	7회	8회	9회	10회
100만원	200만원	300만원	400만원	500만원	600만원	700만원	800만원	900만원	1,000만원

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
아. 법 제25조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 처리위탁에 관한 사항을 공개하지 않거나 알리지 않은 경우	법 제76조 제2항제1호	600	1,200	2,000
자. 법 제25조제6항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리위탁을 할 때에 문서에 의하지 않은 경우	법 제76조 제3항제2호의5	300	600	1,000
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 정보 제공 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.

33 이에 따라 정보통신망법 제27조의3제1항 및 제28조제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하므로 기준금액의 30%인 300만원을 각 가중한다.

< 과태료 부과지침 [별표2] ‘과태료의 가중기준’ >

기준	가중사유	가중비율
위반의 정도	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 2분의 1까지 감경할 수 있다고 규정하고 있다.

34 이에 따라 조사 과정 중 법규 위반 행위를 중지하고 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 정보통신망법 제25조제2항, 제25조제6항, 제28조제1항 위반행위에 대해 기준금액의 50%인 300만원, 150만원, 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§25②	600만원	없음	300만원	300만원
§25⑥	300만원	없음	150만원	150만원
§27의3①	1,000만원	300만원	없음	1,300만원
§28①2·3호	1,000만원	300만원	500만원	800만원
계				2,550만원

다. 최종 과태료

35 이에 따라 피심인의 정보통신망법 제25조제2항·제6항, 제27조의3제1항, 제28조제1항 위반행위에 대해 25,500,000원의 과태료를 부과한다.

VI. 결론

36 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제2호의3·제3호(과태료), 제76조제2항제1호(과태료), 제76조제3항제2호의5(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 4월 29일

위원장 한 상 혁



부위원장 표 철 수

(인)

위 원 허 욱



위 원 김 창 룡

기차
무인
(인)

위 원 안 형 환

(원)