방 송 통 신 위 원 회
심의·의결

안건번호 제2020-23-105호

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

가. 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소할 것

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

다. 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

라. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

마. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것

바. 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것

3. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

4. 피심인은 만 14세 미만의 아동으로부터 개인정보를 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 다음과 같은 방법으로 법정

대리인이 동의하였는지를 확인하여야 한다.

가. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자등이 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법

나. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법

다. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통해 본인 여부를 확인하는 방법

라. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법

마. 동의 내용이 적힌 전자우편을 발송하여 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법

바. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 얻거나 인터넷 주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법

사. 그 밖에 가항부터 바항까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

5. 피심인은 제1항부터 제4항까지의 시정명령을 받은 사실을 시정명령을 받은

날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 애플리케이션에 1주일 이상 게시하여야 한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

6. 피심인은 제1항부터 제5항까지의 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.

7. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

가. 과 징 금 : 22,800,000원

나. 과 태 료 : 18,000,000원

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 온라인 정액제 서비스(, 모바일 앱 ' ')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('18.12.말 기준)

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 천원)

구 분	2016년	2017년	2018년	평 균
정보통신 매출액				*

※ 매출액 : 피심인이 제출한 자료, 사업개시 :

* 사업개시 후 '18년 말까지의 매출액을 연평균 매출액으로 환산한 금액

Ⅱ. 사실조사 결과

1. 조사 대상

2 방송통신위원회는 개인정보보호 포털(i-privacy.kr, KISA)에 유출 신고한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2019. 6. 27. ~ 6. 28.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집 · 이용 현황

3 피심인은 정액제 서비스( )를 2017. 2. 15.부터 운영하면서 2019. 6. 27. 기준 건의 이용자 정보를 수집 · 보관하고 있다.

< 개인정보 수집 · 이용 현황 >

구분	항목	수집일	건수
이용자 정보	(필수) 간편로그인 정보 (선택) 별명, 이메일, 생년월일, 핸드폰 번호, ID, PW		건
총 계			건

나. 개인정보 유출 규모 및 항목

4 피심인의 홈페이지( ) 회원 이메일주소 117,800건이 유출되었다.

다. 유출 경위

5 피심인이 운영하는 도서 정액제 서비스 홈페이지( ) 내 검색 기능( )에 SQL Injection 취약점이 존재하여, 미상의 해커(이하 참고1에서 '이 사건의 해커'라 한다.)에 의해 2019. 6. 14. 18:08부터 해당 취약점을 통해 회원 이메일 117,800건이 외부로 유출되었다.

※ 웹 서버에서는 접근하는 IP에 대한 로그를 남기고 있지 않아, 공격을 수행한 IP 정보 확인이 불가능

< 개인정보 유출 증적 , 이 사건의 해커가 실행한 SQL 인젝션 쿼리 마지막 부분 >

라. 개인정보 유출 대응

일시		피심인의 유출 인지·대응 내용
'19. 6. 17.	12:00	서비스 DB 장애로 인해 DB서버 이상 징후 확인
	14:00	DB서버 원인 분석 중 웹 서버에서 이상 DB Query 발생 확인
	18:00	DB Query 분석을 통해 회원 이메일에 대한 부정 접근·**유출 인지**
'19. 6. 18	11:40	개인정보보호 포털(i-privacy.kr)에 개인정보 **유출 신고**
	16:38	홈페이지에 개인정보 유출에 관한 안내사항 공지
'19. 6. 19	10:33	전체 회원을 대상으로 개인정보 **유출 통지** 메일 발송

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 고객센터 운영 등 민원 대응을 목적으로 ' ' 회사에 개인정보 처리 위탁을 하고 있으나, 이용자에게 개인정보 처리 위탁(위탁 받는 자, 위탁하는 업무 내용)에 대하여 이용자 안내 및 동의를 받은 사실이 없으며 개인정보처리방침에도 관련 사항을 공개하지 않은 사실이 있다.

< 피심인이 개인정보처리방침에 공개한 개인정보 처리 위탁 업체 >

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

7 **(접근권한 부여·말소)** 피심인은 서비스 이용자의 개인정보를 처리하는 관리자 페이지( )의 접근 권한이 있는 개인정보취급자 계정 중 퇴사자 7명의 계정을 말소하지 않은 사실이 있다.

< 피심인의 개인정보취급자 명단 중 퇴사자 계정 >

※ 이메일 주소가 공란인 부분은 퇴사자 계정임

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

9 **(침입탐지 및 침입차단시스템 설치·운영)** 피심인은 정액제 서비스( )를 운영하면서 AWS(아마존 클라우드 서비스) 내 존재하는 IP 제한 기능만을 이용하여 서비스를 운영하고 있었으며, IPS·웹 방화벽 등 별도의 보안 장비를 운영하지 않은 사실이 있다.

10 **(개인정보 유·노출 방지 조치)** 피심인은 자체 제작하여 운영하고 있는 홈

페이지에 대하여 모의 해킹 및 취약점 점검 등을 수행하지 않고 웹 취약점이 존재하는 검색 페이지(　　)를 운영한 사실이 있다.

< 웹 취약점이 존재하는　　파일 소스 일부 >

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}

11 피심인은 개인정보처리시스템의 개인정보취급자에 대한 접속기록을 보관·확인·감독해야하나, 개인정보취급자의 ID, 수행 업무에 대한 정보를 기록하지 않고 있으며, 기록하고 있는 접속한 IP에 대해서도 별도의 확인·감독을 하지 않은 사실이 있다.

< 피심인의 접속기록(취급자의 ID 및 수행업무)이 누락 화면 >

라. 개인정보의 암호화를 소홀히 한 행위{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}

12 피심인은 개인정보를 처리하는 관리자 페이지( )를 운영함에 있어서 로그인부터 개인정보처리의 모든 과정에서 HTTPS 암호화 프로토콜을 운영하지 않고 있으며, 전송구간 암호화를 위해 별도의 암호 알고리즘을 적용하지 않고 일반적인 HTTP 프로토콜로 평문 전송을 한 사실이 있다.

< 피심인의 관리자 페이지 전송구간 캡쳐 화면- ID 및 PW를 평문 전송 중 >

마. 서비스를 이용하지 않은 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

13 피심인은 부터 정액제 서비스( )를 운영하면서 2019. 6. 27. 조사일 기준 최근 1년 동안 로그인하지 않은 회원 95,379건에 대하여 별도 분리보관하거나 파기하지 않고 일반 회원정보와 동일한 DB에서 운영한 사실이 있다.

< 최근 1년 동안 로그인하지 않은 회원 검색결과 >

바. 만14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받지 않은 행위{정보통신망법 제31조(법정대리인의 권리) 중 법정대리인의 동의}

14 피심인은 부터 정액제 서비스( )를 운영하면서 회원가입(SNS 회원가입) 시 14세 미만, 이상 여부를 확인하지 않고 개인정보를 수집하고 있으며, 별도 법정대리인 동의 절차를 운영하지 않은 사실이 있다.

< 피심인의 결제 데이터 중 만14세 미만 인원 수 답변 내용 >

사. 처분의 사전통지 및 의견 수렴

15 방송통신위원회는 2019. 8. 19. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 8. 27. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제25조제1항은 "정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 있도록 업무를 위탁(이하"개인정보 처리위탁"이라 한다)하는 경우에는 '개인정보 처리위탁을 받는 자(이하 "수탁자"라 한다)(제1호)', '개인정보 처리위탁을 하는 업무의 내용(제2호)' 모두를 이용자에게 알리고 동의를 받아야 한다."라고 규정하고 있으며 제2항은 "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 있다.

16 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.

17 '정보통신망법 해설서'는 "법 제25조제1항에 대해 정보통신서비스 제공자등이 제3자에게 개인정보 취급(수집・보관・처리・이용・제공・관리・폐기 등)

업무를 위탁하여 처리할 경우, ①개인정보 취급을 위탁받는 자(수탁자)와 ②개인정보취급위탁의 업무 내용에 대해 이용자에게 고지하고 동의를 얻어야 합니다."라고 설명하고 있으며,

18 또한 "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 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)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'을 하여야 한다."라고 규정하고 있다.

19 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)', '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

20 시행령 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.

21 시행령 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치(제3호)'를 하여야 한다."라고 규정하고 있다.

22 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제2항은 "정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다."라고 규정하고 있으며, 제3항은 "정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다."라고 규정하고 있고, 제5항은 "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 있다.

23 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.

24 고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보

처리시스템에 접속한 기록을 월1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상* 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

* 2020.1.2. 시행된 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호)에서는 접속기록을 최소 1년 이상 보존·관리하도록 개정됨

25 고시 제6조제3항은 "이용자의 개인정보 및 인증정보를 송수신할 때는 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나(제1호), 웹서버에 암호화 응용프로그램을 설치하여(제2호) 전송하는 정보를 암호화하여 송수신하는 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다."라고 규정하고 있다.

26 '고시 해설서'는 고시 제4조제2항에 대해 정보통신서비스 제공자등은 개인정보취급자가 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 개인정보처리시스템에 사용자계정 등 접근권한의 변경·말소 등이 필요할 때에는 정당한 사유가 없는 한 즉시 조치하여야 하며, 불완전한 접근권한의 변경 또는 말소 조치로 인하여 정당한 권한이 없는 자가 개인정보처리시스템에 접근될 수 없도록 하여야 한다고 해설하고 있으며, 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

27 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, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생

한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안운영체제(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 해설하고 있다.

28 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,

29 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.

30 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.

31 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.

다. 정보통신망법 제29조제2항은 "정보통신서비스 제공자등은 정보통신서비스를 1년의 기간동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다."라고 규정하고 있다.

32 정보통신망법 시행령 제16조제2항은 "정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다."라고 규정하고 있다.

라. 정보통신망법 제31조제1항은 "정보통신서비스 제공자등이 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의하였는지를 확인하여야 한다. 이 경우 정보통신서비스 제공자는 그 아동에게 법정대리인의 동의를 받거나 법정대리인이 동의하였는지를 확인하기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다."라고 규정하고 있다.

33 정보통신망법 시행령 제17조의2제1항은 "정보통신서비스 제공자등은 법 제31조제1항에 따라 '동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자등이 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법(제1호)', '동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법(제2호)', '동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리

인의 휴대전화 본인인증 등을 통해 본인 여부를 확인하는 방법(제3호)', '동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법(제4호)', '동의 내용이 적힌 전자우편을 발송하여 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법(제5호)', '전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법(제6호)', '그 밖에 제1호부터 제6호까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법(제7호)'에 해당하는 방법으로 법정대리인이 동의했는지를 확인해야 한다."고 규정하고 있으며, 제2항은 "정보통신서비스 제공자등은 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 법정대리인에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내할 수 있다."고 규정하고 있다.

34 '개인정보 최소 수집·보관 및 이용자 권리 보장을 위한 온라인 개인정보 처리 가이드라인(2018.9.)'은 정보통신망법 제31조'만14세 미만 아동 여부 확인'에 대해 "인터넷 회원가입 단계에서 만14세 미만 아동 여부를 확인하기 위해 필요한 경우에는 이용자가 '법정 생년월일'을 직접 입력하도록 하거나 '만14세 이상'이라는 항목에 체크하도록 하는 등의 조치를 취하고, 사업자는 이를 토대로 만14세 미만인지 여부를 확인하는 것이 바람직함"라고 설명하고 , "다만 만 14세 미만 아동을 주요 대상으로 하여 서비스를 제공하는 사업자의 경우에는 신뢰할 수 있는 방법으로 본인여부를 확인한 후 반드시 법정대리인의 동의를 받아야 함"라고 설명하고 있다.

마. 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}

35 피심인이 고객센터 운영 등 민원 대응을 목적으로 '웅진'회사에 개인정보처리위탁하고 있으나 개인정보처리방침에 개인정보 처리위탁 업무내용 및 수탁자등을 공개하거나 전자우편·서면·모사전송·전화 등을 통해 이용자에게 알리지 않은 행위는 정보통신망법 제25조제2항을 위반한 것이다.

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

36 **(접근권한 부여·말소)** 피심인이 개인정보취급자 계정 중 퇴사자 7명의 계정을 말소하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제2항을 위반한 것이다.

37 **(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.

38 **(침입탐지 및 침입차단시스템 설치·운영)** 피심인이 개인정보처리시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 및 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 침입탐지시스템을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

39 **(개인정보 유·노출 방지 조치)** 피심인이 홈페이지에 대하여 모의 해킹 및 취약점 점검 등을 수행하지 않고 웹 취약점이 존재하는 서비스를 운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제9항을 위반한 것이다.

다. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

40 피심인이 개인정보처리시스템에 접속한 개인정보 취급자의 접속기록(식별자, 접속일시, 접속지, 수행업무)을 기록하여 월1회 이상 정기적으로 확인·감독하지 않고, 그 기록을 최소 6개월 이상 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

라. 개인정보의 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

41 피심인이 개인정보를 처리하는 관리자 페이지( )에서 개인정보(아이디, 비밀번호)를 정보통신망을 통해 송·수신할 때 암호화하지 아니한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제3호, 고시 제6조제3항을 위반한 것이다.

마. 서비스를 이용하지 않은 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

42 피심인이 2019. 6. 27. 조사일 기준 최근 1년 동안 로그인하지 않은 회원 95,379건에 대하여 별도 분리 보관하거나 파기하지 않고 일반 회원 정보와 동일한 DB에서 운영한 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16

조제2항을 위반한 것이다.

바. 만14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받지 않은 행위{정보통신망법 제31조(법정대리인의 권리) 중 법정대리인의 동의}

43 피심인이 회원가입 단계에서 만14세 미만, 이상 여부를 확인하는 절차 없이 개인정보를 수집하여, 만14세 미만 이용자에 대해 법정대리인의 동의를 받지 않고 개인정보를 수집한 행위는 정보통신망법 제31조제1항, 같은 법 시행령 제17조의2제1·2항을 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
	접근 통제	§28①2호	§15②1호	전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경·말소하지 않은 행위(고시§4②)
	접근 통제	§28①2호	§15②1호	개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④3호	이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위(고시§6③)
	유효 기간	§29②	§16②	1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위
	법정대리인의 동의	§31①	§17의2①·②	만14세 미만 여부를 확인하는 절차 없이 개인정보를 수집하여 만14세 미만 이용자에 대해 법정대리인의 동의를 받지 않고 개인정보를 수집한 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 정보통신서비스 제공자로서 제3자에게 이용자의 개인정보를 처리 할 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 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다. 1)개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소할 것 2)개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관할 것 3)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 4)취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것 5)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것 6)정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화할 것

다. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

라. 피심인은 만 14세 미만의 아동으로부터 개인정보를 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 다음과 같은 방법으로 법정대리인이 동의하였는지를 확인하여야 한다. 1)동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자등이 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법 2)동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법 3)동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통해 본인 여부를 확인하는 방법 4)동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법 5)동의 내용이 적힌 전자우편을 발송하여 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법 6)전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법 7)그 밖에 1호부터 6호까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

마. 피심인은 가항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지와 모바일 애플리케이션에 1주일 이상 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

<표> 시정명령 공표(안)

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경·말소하지 않은 행위 ②개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위③개인정보처리시스템에 대한 침입차단 및 침입탐지시스템 운영을 소홀히 한 행위 ④홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위 ⑤개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위 ⑥이용자의 개인정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 암호화하지 아니한 행위 ⑦만 14세 미만 아동의 개인정보 수집·이용·제공 등의 동의 시 법정대리인의 동의를 받지 아니한 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

44 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. 과징금 부과

45 피심인은 정보통신망법 제64조의3제1항제6호에 따라 이용자의 개인정보가 유출된 경우로서 개인정보 보호조치(제28조제1항)를 하지 않은 경우에 해당하고, 정보통신망법 제64조의3제1항제7호에 따라 법정대리인의 동의를 받지 않고 만14세 미만인 아동의 개인정보를 수집한 경우에도 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 각 부과할 수 있다.

46 피심인의 정보통신망법 제28조제1항 및 제31조제1항 위반에 대한 과징금은 같은 법 제64조의3제1항제6호·제7호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정 기준과 산정절차) 및 '개인정보보호 법규 위반에 대

한 과징금 부과기준(방송통신위원회 고시 제2015-30호, 이하 '과징금 부과기준 '이라 한다)' 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

47 피심인의 정보통신망법 제28조제1항 및 제31조제1항 위반에 대한 과징금 상한액은 같은 법 제64조3의제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2016년	2017년	2018년	3년 평균
관련 매출액				*

※ 자료출처 : 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

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

나. 기준금액

1) 고의·중과실 여부

48 과징금 부과기준 제5조제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

49 이에 따를 때, ▲정보통신망법 제28조제1항제2호에 따른 접근통제 중 홈페

이지에 대해 취약점 점검과 그에 따른 조치를 수행하지 않은 피심인에게 이용자의 개인정보 유출에 대한 중과실이 있다고 판단하며, ▲영리를 목적으로 법정대리인의 동의 없이 만14세 미만 아동의 개인정보를 수집·이용한 피심인에게 중과실이 있다고 판단한다.

2) 중대성의 판단

50 과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있고,

51 과징금 부과기준 제5조제3항 단서조항은, 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 규정하고 있다.

판단기준	- 사업자에게 고의·중과실이 있어 '매우 중대한 위반행위'로 판단되나 아래 사항 중 1개이상 2개이하인 경우 '중대한 위반행위'에 해당 ①위반행위로 직접적 이득을 취득하지 않은 경우 ②피해규모가 보유하고 있는 개인정보의 100분의 5 이내인 경우 ③이용자의 개인정보가 공중에 노출되지 않은 경우
적용근거	- 위반행위로 직접적 이득은 취득하지 않았다는 점(개인정보 보호조치) - 피해규모가 100분의 5 이내인 점(법정대리인 동의)

52 이에 따라, 피심인의 위반행위의 결과가 ▲개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점, ▲법정대리인의 동의 없이 수집한 만 14세 미만 아동의 개인정보의 수가 보유하고 있는 개인정보의 100분의 5 이내인 점 등을

종합적으로 고려할 때, 각 위반행위의 대성을 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

53 피심인의 정보통신부문 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 각 원으로 한다.

<정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

54 과징금 부과기준 제6조와 제7조에 따라 개인정보 보호조치 관련 위반기간이 1년 이내(19.6.14.~.6.27.)이므로 가중 없이 기준금액을 유지하고, 법정대리인 동의 관련 위반기간은 2년 초과(~'19.7.9.)에 해당하여 기준금액의 100분의 50에 해당하는 원을 가중하고,

55 최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 원을 각 감경한다.

라. 추가적 가중 및 감경

56 과징금 부과기준 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조

사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

57 이에 따를 때, 피심인이 ▲개인정보 유출사실을 자진 신고한 점, ▲조사에 성실히 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 원과 원을 각 감경한다.

2. 과징금의 결정

58 피심인의 정보통신망법 제28조(개인정보의 보호조치) 및 제31조(법정대리인의 권리) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액은 각 원과 원이나 과징금 산출액이 1억원 미만에 해당하여 십만원 미만을 절사하여 최종과징금은 각 7,600,000원과 15,200,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

사업자명	기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
	천원 (중대한 위반) ※ 개인정보 보호조치	① 기준금액 유지(단기위반) ② 기준금액의 50% 감경 (최초위반 : 천원)	필수적 가중·감경 거친 금액의 20% 감경 (천원)	**760만원**
	천원 (중대한 위반) ※ 법정대리인 동의	① 기준금액의 50% 가중 (장기위반 : 천원) ② 기준금액의 50% 감경 (최초위반 : 천원)	필수적 가중·감경 거친 금액의 20% 감경 (천원)	**1,520만원**
합 계				**2,280만원**

* '전기통신사업법 금지행위 위반에 대한 과징금 산정 실무요령'에 따라 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

Ⅵ. 과태료 부과

59 피심인의 정보통신망법 제25조(개인정보의 처리위탁)제2항, 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 제76조제2항제1호, 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

60 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 정보통신망법 제25조제2항 위반에 대한 기준금액은 1회 위반 과태료인 600만원을 적용하고, 정보통신망법 제28조제1항 및 제29조제2항 위반에 대한 기준금액은 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
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
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
더. 법 제29조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 하지 아니한 자	법 제76조 제1항제4호	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.

61 이에 따라 정보통신망법 제28조제1항 위반행위에 대해 세부기준에서 정한 행위가 3개 이상인 경우에 해당하므로 기준금액의 50%인 500만원을 가중하고 정보통신망법 제25조제2항 및 제29조제2항 위반행위에 대해서는 특별히 가중할 사유가 없으므로 기준금액을 각 유지한다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

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

위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

62 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 위반행위에 대해 기준금액의 50%인 300만원을 감경하고 정보통신망법 제28조제1항 및 제29조제2항 위반행위에 대해서는 기준금액의 50%인 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§25②	600만원	없음	300만원	**300만원**
§28①2·3·4호	1,000만원	500만원	500만원	**1,000만원**
§29②	1,000만원	없음	500만원	**500만원**
계				**1,800만원**

다. 최종 과태료

63 이에 따라 피심인의 정보통신망법 제25조제2항, 제28조제1항, 제29조제2항 위반행위에 대해 18,000,000원의 과태료를 부과한다.

Ⅶ. 결론

64 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호·제7호(과징금) 및 제76조제1항제3호·제4호(과태료), 제76조제2항제1호(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

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)