방 송 통 신 위 원 회
심의·의결

안건번호 제2020-23-106호

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 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.

2. 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.

3. 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 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것

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

라. 비밀번호는 복호화 되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것

4. 피심인은 이용자의 동의를 받은 개인정보의 수집 및 이용·목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

5. 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.

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 과태료를 부과한다.

가. 금　　액 : 31,000,000원

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

채널을 운영하는 방송채널사용사업자로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제67조에 따라 시청자의 개인정보를 수집·이용하는 경우로, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수('19.9.2. 기준)

< 피심인의 최근 3년간 매출액 현황 >

(단위 : 천원)

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

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

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. 7. 10. ~ 7. 11.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집 · 이용 현황

3 피심인은 방영프로그램 정보 및 이벤트 등을 위한 사이트( ) 등을 운영하면서 2019.7.10. 기준 건의 이용자 정보를 수집 · 보관하고 있다.

< 개인정보 수집 · 이용 현황 >

구분	항목	수집일	건수
이용자 정보	아이디, 비밀번호, 주민등록번호, 성명, 주소, 전화번호, 이메일, 생년월일, 성별	~ '19.7.10.	건
총 계			건

나. 유출 규모 및 항목

4 홈페이지 회원의 개인정보(아이디, 비밀번호*, 주민등록번호**, 성명, 주소, 전화번호, 이메일, 생년월일, 성별 등) 56,276건이 외부로 유출되었다.

* 비밀번호는 BASE64(숫자를 이용하여 데이터를 64bit길이로 변환하는 함수)로 인코딩되어 있음

** 주민등록번호는 SHA-1을 2회 암호화하여 생성된 해쉬값

< 피심인의 개인정보 유출 현황 >

구분	유 출 항 목	건 수
홈페이지 회원	아이디, 비밀번호, 주민등록번호, 성명, 주소, 전화번호, 이메일, 생년월일, 성별 등	56,276건

다. 유출 경위

5 애니맥스 홈페이지 이용자 정보(아이디, 비밀번호 등)가 담긴 backup.sql 파일이 인터넷 환경에서 다운로드 될 수 있는 상태(URL : /backup.sql)로 2013. 8. 30. 업로드되어 권한 없는 IP인 185.51.61. (러시아, 2019. 5. 8. 21:15)와 197.58.251. (이집트, 2019. 5. 8. 22:52)에서 개인정보가 담긴 파일(backup.sql)이 외부로 다운로드 되었다.

라. 개인정보 유출 대응

일시	피심인의 개인정보 유출 인지·대응 내용
2019. 5. 9.	모회사(본사)에서 보안 모니터링 과정에서 홈페이지 취약점 발견
2019. 6. 11. 17:17	모회사는 로그분석을 통해 권한 없는 IP(185.51.61. , 197.58.251.)에서 backup.sql 파일을 다운로드한 로그기록을 확인
2019. 6. 12. 16:25	개인정보보호 포털(i-privacy.kr)에 개인정보 **유출 신고**
2019. 6. 15. 16:42	유출사실을 이메일로 **이용자에게 통지**

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 주민등록번호를 수집·이용한 행위{정보통신망법 제23조의2(주민등록번호의 사용제한)}

6 피심인은 유출 파일 기준으로 ~ 2013. 2. 15. 수집한 주민등록번호 54,874건을 보관한 사실이 있다.

< 피심인이 암호화하여 보관중인 주민등록번호 일부 >

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

7 피심인은 2019. 6. 11.에 유출사실을 인지하였으나, 4일이 지난 2019. 6. 15. 이용자에게 개인정보 유출사실을 이메일로 통지하였으며, 이메일 통지 외에 홈페이지 등에 유출사실을 공개한 사실은 없었다.

<피심인의 개인정보 유출 통지 메일 발송 결과>

※ 유출안내를 위해 발송된 이메일 53,946건 중 발송 실패한 건수는 23,225(43%)이나, 개인정보 유출사실에 대하여 홈페이지 공지 등 추가로 알리지 않음

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

8 **(침입차단 시스템 설치·운영)** 피심인은 개인정보처리시스템에 대해 침입탐지시스템인 웹방화벽(SSG-5 주니퍼)을 설치·운영하고 있었으나, 개인정보 침입차단시스템을 설치·운영하지 않은 사실이 있다.

< 피심인의 네트워크 구성도>

9 **(개인정보 유·노출 방지 조치)** 피심인은 개인정보가 담긴 파일을 인터넷망에서 접근 할 수 있는 위치(/backup.sql)에 저장하여 허가받지 않은 자의 접근을 허용한 사실이 있다.

<다운로드 가능한 위치에 업로드 된 backup.sql 파일>

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

10 피심인은 개인정보처리시스템 접속기록을 2014.7.22.부터 ID, 접속일시, IP를 기록하고 있으나, 열람, 삭제 등의 수행내역을 기록하여 보관하지 않은 사실이 있다.

< 피심인의 접속기록 화면 - 수행내역은 기록하지 않음 >

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

11 피심인은 이용자의 비밀번호를 암호화하지 않고 인코딩(BASE64*)하여 DB에 저장한 사실이 있다.

* BASE64 : 데이터를 숫자를 이용하여 64비트 길이로 변환하는 함수로 역변환이 가능함

< DB에 저장중인 이용자의 비밀번호 - 암호화하지 않고 단순 인코딩방식으로 저장 >

바. 수집·이용 목적이 달성된 개인정보를 파기하지 아니한 행위 {정보통신망법 제29조(개인정보의 파기)중 목적을 달성한 경우}

12 피심인은 부터 2016.06.29.까지 탈퇴 신청한 이용자 2,518명의 이름, 아이디, 탈퇴신청일 등의 개인정보를 파기하지 않고 테이블에 보관한 사실이 있다.

< 테이블에 보관중인 개인정보 수 - 2,518건 >

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

13 피심인은 홈페이지( ) 마지막 접속일시가 2018. 7. 1. 이전인 이용자 개인정보 10,068건을 파기하거나 별도 분리 보관하지 않은 사실이 있다. (2019. 7. 10. 기준)

< 최종 접속일이 2018.7.1. 이전인 이용자 수(10,068건) 화면 >

아. 처분의 사전통지 및 의견 수렴

14 방송통신위원회는 2019. 8. 19. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 9. 2. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제23조의2제1항은 "정보통신서비스 제공자는 '본인확인기관으로 지정받은 경우(제1호)', '법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우(제2호)', '영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우(제3호)'를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다."라고 규정하고 있다.

15 정보통신망법 제23조의2제1항제3호에 따라 고시한 「영업상 목적을 위하여

이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자 고시」 제1조는 "「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2제1항 제3호에서 "영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자"라 함은 전기통신사업법 제38조 제1항 또는 제2항에 따라 기간통신사업자로부터 이동통신서비스를 도매 제공 받아 재판매하는 전기통신사업자를 말한다. 다만, 본문의 영업상 목적이란 이동전화번호를 이용한 본인확인 서비스를 말한다."라고 규정하고 있다.

16 「정보통신망법 해설서」는 법제23조의2제1항에 대해 본인확인기관이거나 법령이나 고시에서 주민등록번호의 수집·이용을 허용하는 경우가 아니면 주민등록번호를 수집·이용할 수 없으며, 기존에 보유하고 있는 주민등록번호도 법령 시행 후 2년 이내 파기하도록 하고 있어 2014년 8월 이전까지 삭제하여야 한다고 해설하고 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.

17 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·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.

18 '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)', '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 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등을 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 있으며, 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)'을 하여야 한다."라고 규정하고 있다.

20 시행령 제15조제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."라고 규정하고 있다.

21 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 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, 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.

22 고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 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

23 고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

24 '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 해설하고 있다.

25 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,

26 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.

27 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 있으며,

28 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 ⅰ)식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), ⅱ)접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시

점) 〈년-월-일, 시:분:초〉, iii)접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), iv)수행업무(개인정보처리시스템에서 개인정보취급자가 처리한 내용을 알 수 있는 정보) 〈개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위〉 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다고 해설하고 있다.

29 고시 제6조제1항에 대해 정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조되지 않도록 개인정보처리시스템, 업무용컴퓨터, 보조저장매체 등에 개인정보취급자 및 이용자 등이 입력한 비밀번호를 평문형태가 아닌 해쉬함수를 통해 얻은 결과 값으로 시스템에 저장(일방향 암호화)하여야 한다고 해설하고 있다.

라. 정보통신망법 제29조제1항은 "정보통신서비스 제공자등은 '제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다."라고 규정하고 있으며, 제23조제1항 단서는 "다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다."라고 규정하고 있다.

30 정보통신망법 제29조제2항은 "정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다."라고 규정하고 있다.

31 정보통신망법 시행령 제16조제2항은 "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.

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. 주민등록번호를 수집·이용한 행위{정보통신망법 제23조의2(주민등록번호의 사용제한)}

32 피심인이 부터 2013. 2. 15.까지 수집한 이용자의 주민등록번호 54,874건을 파기하지 않고 보관한 행위는 정보통신망법 제23조의2제1항을 위반한 것이다.

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

33 피심인이 개인정보 유출사실을 인지한 후 4일이 지난 2019. 6. 15. 이용자에게 유출사실을 통지한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

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

34 **(침입차단 시스템 설치·운영)** 피심인이 개인정보처리시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

35 **(개인정보 유·노출 방지 조치)** 피심인이 개인정보가 담기 파일을 인터넷망에서 접근 할 수 있는 위치에 저장하여 허가받지 않은 자의 접근을 허용한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

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

36 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무 확인 등을 위해 식별자, 접속일시, 접속지, 수행업무 등을 포함하는 접속기록을 6개월 이상 보관하여야 하나, 피심인이 접속기록에 열람, 삭제 등의 개인정보취급자의 수행내역을 누락하여 보관한 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

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

37 피심인이 이용자의 비밀번호를 안전한 해쉬함수(보안강도 112비트 이상)로 암호화하여 저장하지 않고 인코딩(BASE64)방식으로 DB에 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

바. 수집·이용 목적이 달성된 개인정보를 파기하지 아니한 행위{정보통신망법 제29조(개인정보의 파기)중 목적을 달성한 경우}

38 피심인이 2008. 12. 18.부터 2016. 6. 29.까지 탈퇴 신청한 이용자 2,518명의 이름, 아이디, 탈퇴신청일 등의 개인정보를 즉시 파기하지 않고

테이블에 보관한 행위는 정보통신망법 제29조제1항을 위반한 것이다.

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

39 피심인이 1년간 홈페이지에 로그인 기록이 없는 이용자의 개인정보 10,068건을 파기하거나 별도 분리 보관하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	주민등록번호	§23의2①		법적 근거 없이 이용자의 주민등록번호를 수집·이용한 행위
	지연 신고	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단시스템을 설치·운영하지 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 접속기록 작성 시 수행업무를 누락하여 저장·보관한 행위(고시§5①)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 안전하지 않은 암호화 알고리즘으로 암호화 하여 저장한 행위(고시§6①)
	미파기	§29①		동의받은 개인정보의 보유·이용기간이 지난 개인정보를 파기하지 않고 보관한 행위
	유효 기간	§29②	§16②	1년간 로그인 기록이 없는 회원의 개인정보를 파기 또는 별도 분리·보관하지 않은 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.

나. 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.

다. 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 3)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것 4)비밀번호는 복호화 되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것

라. 피심인은 이용자의 동의를 받은 개인정보의 수집 및 이용·목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

마. 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.

2. 시정명령 이행결과의 보고

40 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

41 피심인의 정보통신망법 제23조의2(주민등록번호의 사용 제한)제1항, 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항에 대한 과태료는 같은 법 제76조제1항제2호·제2호의3·제3호·제4호, 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

42 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 각 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
다. 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	법 제76조 제1항제2호	1,000	2,000	3,000
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
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.

43 이에 따라 정보통신망법 제28조제1항에 대해 세부기준에서 정한 위반행위가 3개 이상인 경우에 해당하므로 기준금액의 50%인 500만원을 가중한다.

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

44 이에 따라 정보통신망법 제23조의2제1항 및 제27조의3제1항 위반행위에 대해 중기업으로 평균 당기순이익이 적자인 점을 고려하여 기준금액의 20%인 200만원을 각 감경하고 정보통신망법 제28조제1항 및 제29조제2항 위반행위에 대해 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 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§23의2①	1,000만원	없음	200만원	**800만원**
§27의3①	1,000만원	없음	200만원	**800만원**
§28①2·3·4호	1,000만원	500만원	500만원	**1,000만원**
§29②	1,000만원	없음	500만원	**500만원**
계				**3,100만원**

다. 최종 과태료

45 이에 따라 피심인의 정보통신망법 제23조의2제1항, 제27조의3제1항, 제28조제1항, 제29조제2항 위반행위에 대해 31,000,000원의 과태료를 부과한다.

Ⅵ. 조사결과 수사기관 이첩

46 정보통신망법 제29조(개인정보의 파기)제1항제1호에 따라 정보통신서비스 제공자등은 이용자에게 동의받은 개인정보의 수집·이용 목적 등을 달성한 경우 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 이를 위반하는 경우 같은 법 제73조제1의2호에 따라 2년 이하의 징역 또는 2천만원 이하의 벌금에 해당한다.

47 피심인은 조사당시까지 수집·이용 목적 등을 달성한 이용자의 개인정보 2,518건을 파기하지 않고 보유하고 있어 정보통신망법 제29조(개인정보의 파기)제1항제1호를 위반하는 행위가 있다고 인정된다. 이에 같은 법 제73조제1의2호에 해당되어 조사결과를 수사기관에 이첩한다.

Ⅶ. 결론

48 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제2호·제2호의3·제3호·제4호(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)