방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 38 - 170호

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 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 기

술적·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. 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

마. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것

바. 개인정보처리시스템에 접근 할 수 있는 개인정보취급자의 비밀번호는 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성, 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고, 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하는 사항 등을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용할 것

사. 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

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

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

차. 이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리듬으로 암호화하여 저장 할 것

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

4. 피심인은 제1항부터 제3항까지의 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.

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 과징금 및 과태료를 부과한다.

가. 과 징 금 : 494,000,000원

나. 과 태 료 : 33,000,000원

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 도메인 등록, 웹호스팅, 홈페이지 구축 등 IT서비스 상품안내 및 신청 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
관련 매출액				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

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. 5. 21.~5. 22., 7. 29.~7. 30.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 도메인 등록, 웹호스팅, 홈페이지 구축 등 IT서비스 상품안내 및 신청 사이트 를 부터 운영하면서 2019. 5. 20.기준 이용자 620,529건의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
회원정보 (유효회원)	(필수) 아이디, 비밀번호, 이름, 이메일, 휴대전화 (선택) 전화번호, 주소, 팩스, 세금계산서 정보, IPIN번호(IPIN 가입시) (선택) 주민등록번호, 신분증		건
(휴면회원)	상동		건
총계			**건**

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019.4.23. 피심인의 직원이 금융업무 이용 중 금융보안프로그램에서 비정상

네트워크 행위가 탐지된 사실을 사내 보안팀에 제보하여 사내 악성코드 감염 인지함

- 2019.4.25. 피심인은 사내 악성코드 감염 분석 중 그룹웨어 웹하드를 통해 개인정보 파일 유출 인지함
- 2019.4.26. 피심인은 내부 검토를 통해 웹하드 기능을 종료
- 2019.4.29. 긴급회의 소집(고객정보, 서버정보, 피심인의 내부정보 유출 확인)
- 2019.4.29.~5.14. 피심인은 내부 감염 PC 25대를 교체 혹은 포맷 조치함
- 2019.5.02. 행정안전부에 개인정보 유출 신고(1차)
- 2019.5.07. 개인정보 추가 유출 155,039건(일부 중복 포함) 인지
- 2019.5.14. 개인정보 유출 통지 및 홈페이지 공개
- 2019.5.14. 개인정보 유출대상 개인정보 유출 내역 상세 조회 페이지 제공
- 2019.5.15. 방송통신위원회에 개인정보 유출 신고(2차)
- 2019.6.4. 개인정보 유출 건수 추가 분석
- 2019.6.19. 방송통신위원회에 개인정보 유출 신고(3차)

※ 2019.5.7. 인지된 건에 대한 유출 신고 (191,667건, 중복제거시 165,654명)

2) 개인정보 유출 규모

4. 피심인의 이용자 정보 및 호스팅* 이용자 개인정보 191,667건(중복제거시 165,564건)의 개인정보가 유출되었다.

* 2014. 12. 8. 로부터 인수된 호스팅 고객정보 85,190건 포함

< 피심인의 개인정보 유출현황 >

구 분	유 출 항 목	건 수
이용자정보	이름, 아이디, 이동전화번호, 이메일, 생년월일, 성별, 계좌번호, 집주소, 회사주소, 사진, 주민등록번호, 여권번호, 운전면허번호 등	191,667건 (중복제거 시 165,564건)

3) 유출 경로

- 2018. 6. 14. 10:25 피심인이 운영 중인 그룹웨어*
(이하 '그룹웨어'라 한다)의 메일 서비스에 미상의 해커
(61.75. , 221.110. , 111.223. 이하 '이 사건의 해
커'라 한다)가 등 직원 계정으로 접속(POP3**)하여 개인정
보가 포함된 파일을 다운로드하였다.

* 그룹웨어 : 피심인이 직접 개발하여 판매·사용하는 그룹웨어 서비스로 메일, 게시판, 일정관리, 웹하드 등 그룹웨어의 기본적인 기능을 제공하고 있음

** POP3 : 메일 서버에서 이메일을 로컬 장치(이용자의 PC 등)로 다운로드하여 보관하는 메일 서비스 방식

※ 피심인은 POP3를 이용해 외부에서 접속한 계정 및 다운로드한 파일 정보를 분석하지 않음

- 2018. 6. 22. 16:56 이 사건의 해커는 ' ' 계정으로 그룹웨어에 접속하여 그룹웹하드***(이하, '업무용 공유 폴더'라 한다)에 저장·공유된 일부 파일을 다운로드함

*** 그룹웹하드 : 웹하드 접속 시 전 사용자에게 기본적으로 공유되는 폴더로 읽기/쓰기/삭제 권한이 할당됨

- 2018. 11. 5. 12:28 이 사건의 해커는 ' ' 계정으로 업무용 공유 폴더에 접속하여 .zip 파일을 다운로드하였고, 업무용 계정 정보가 평문으로 저장된 파일 ' .txt'을 획득함

- 2018. 11. 5. ~ 2019. 3. 20. 이 사건의 해커는 획득한 계정 정보(
)를 이용해 업무용 공유 폴더 내 개인정보 파일을 지속적 탈취, 약 172,130건의 개인정보가 포함된 파일이 유출됨

※ 2018. 6. 22. ~ 2019. 4. 11. 기간 동안 메일 백업, 업무 백업, 호스팅결제, 인수인계 파일, DB 암호화 설치 프로그램, 결제 ID/PW, 서버 현황, 관리자 계정 관리대장, 구성도, IDC 업무메뉴얼, 회원정보 파일 등을 다운로드 함

- 2019. 1. 10. 16:51 이 사건의 해커는 내부망 공격을 시도하기 위해, ' ' 계정을 이용해 업무용 공유 폴더('경영지원실')에

설치 프로그램* 삭제 후 원격제어 악성코드를 삽입/변조하여 동일 이름으로 다시 업로드함

* 'ms .zip'(압축된 MS 오피스 2010) 및 'SetupAxGateManager_v .exe' (방화벽 관리 프로그램)

- 2019. 2. 15 피심인의 자체 분석 결과, 변조된 'ms .zip' 파일을 피심인의 공인 IP 및 외부 IP에서 31명이 다운로드 하였으며, 12명의 사용자가 PC에서 악성코드가 설치되어 C&C (ws. .com, .com, 103.91.)의 명령을 통해 사내 서버 대역(211.115.)으로 접속(SSH)이 시도된 것으로 파악

※ 피심인은 12대의 PC를 초기화(포맷)하였으며, 해킹 경유지로 이용된 PC에서 서버 대역으로 접속 후 이루어진 행위에 대한 추가 분석은 이루어지지 않음

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 주민등록번호를 수집·이용 한 행위

5. 피심인은 법령상 주민등록번호를 처리할 수 있는 근거가 없음에도 업무 처리를 목적(개인회원의 ID 및 비밀번호 찾기, 이름 개명, 관리 ID변경, 도메인 소유권 이전, 도메인 소유자 정보변경, 네임서버 변경 등)으로 이용자의 신분증 사본을 수집하여 2019.4.29.까지 웹서버 상에 저장·공유하다가 보유하고 있던 주민등록번호가 유출된 사실이 있다.

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

6. 피심인은 2019.4.25. 개인정보 유출사고 인지 후 2019.4.29. 긴급회의 등을 소집하여 개인정보 유출 피해대상·규모 등을 확인하였으나, 24시간을 경과하여 개인정보 유출 신고(2019.5.7.) 및 통지(2019.5.14.)를 하였으며, 피심인이 기 신고한 개인정보 이외에 추가 유출건에 대해 개인정보 유출 신고 및 통지를 실시하지 않은 사실이 있다.

7. 피심인은 2019.4.25. 티티호스팅 고객의 개인정보(85,190건)가 추가 유출된 사실을 인지하였으나, 24시간을 경과하여 이용자에게 개인정보 추가 유출 통지(2019.5.21.) 및 신고(2019.6.19.)한 사실이 있다.

8. 피심인은 자체분석 결과 6개 파일에서 191,667건(중복제거 시 165,654건)이 유출된 것으로 파악하였으나, DB, Outlook 파일 등 다수의 파일이 대상에서 누락된 사실을 확인하고 해당 사실을 인지하였으나 추가적인 개인정보 유출 확인 절차를 진행하지 않은 사실이 있다.

다. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

1) 피심인은 개인정보가 포함된 파일의 공유를 위해 업무용 공유폴더를 사용한 사실이 있으며, 웹하드에 접속 가능한 계정의 접근권한을 사용자 및 부서별로 차등 부여하지 않고, 모든 직원에게 읽기/쓰기/삭제 권한이 할당되도록 운영한 사실이 있다.

2) 피심인은 사내 전체 개인정보취급자의 접근 권한에 부여, 변경, 말소 내역을 5년간 보관 관리해야 하나, 2019.5.21. 조사 당시 개인정보취급자의 접근권한 부여 내역을 관리하지 않았고 2018년도 4분기 1회의 기록만 보관한 사실이 있다.

3) 피심인은 그룹웨어를 운영하면서 개인정보취급자가 외부 인터넷망에서 아이디와 패스워드만으로 접속하여 업무용 공유폴더에 저장·공유 중인 개인정보 파일을 다운로드 되도록 운영한 사실이 있다.

4) 피심인은 2018.3.8.부터 방화벽 및 웹방화벽을 운영하고 있었으나 2018. 6. 14.~2019. 1. 24. 기간 동안 외부 IP에서 POP3(아웃룩 메일), SSH(서버접속)을 통한 대량의 접속이 탐지되었음에도 개인정보 유출 시도를 차단하기 위해 주기적인 접

속 IP 재분석을 통한 IP 차단 등 추가적인 조치를 하지 않은 사실이 있다.

9. 피심인은 2008. 4.~2019. 4. 25. 기간 동안 업무를 목적으로 업무용 공유폴더에 부서별 폴더를 생성하고, 업무상 처리한 개인정보가 포함된 파일을 업무용 공유폴더에 저장·공유하고 있었으나, WEB 및 C/S 프로그램을 통해 외부 인터넷망에서의 접근을 IP 등으로 제한하지 않고 아이디와 비밀번호만으로 접속할 수 있도록 운영한 사실이 있다.

※ 피심인은 그룹웨어 서버(121.254.)로의 외부 접속을 모두 허용(Rule)하고 있었으며, 일부 IP만 한정적으로 차단(Rule)하는 정책을 반영하여, 보안시스템운영절차서_v1.0의 정책을 준수하지 않고 모두 허용 후 일부를 차단하는 정책을 반영한 것으로 확인

5) 피심인은 2008.4.~2019.4.25. 기간 동안 인터넷망에서 업무용 공유폴더에 접속하여 개인정보가 포함된 파일의 다운로드 기능 및 접근 권한 변경기능에 대한 접근을 제한하지 않았으며,

- 2019.5.22. 현장조사 시 개인정보처리시스템에 접속할 수 있는 개인정보취급자의 PC가 외부 인터넷 페이지에 접속이 가능한 사실이 있다.

6) 피심인은 개인정보취급자(내부 직원)를 대상으로 발급한 그룹웨어 계정의 비밀번호 유효기간을 설정하지 않고 운영하다가, 유출 사고 발생 이후인 2019.4.29. 비밀번호 유효기간을 90일로 설정한 사실이 있다.

7) 피심인은 2018.6.22.~2019.3.20. 기간 동안 이 사건의 해커로부터 그룹웨어 웹하드의 업무용 공유폴더에 저장 중인 201개의 파일이 외부로 다운로드 되어, 191,667건(중복제거 시 165,654건)의 개인정보 유출된 사실된 사실이 있으며, 2018.6.14.~2019.1.24. 기간 동안 POP3를 통해 개인정보 파일이 다운로드된 사실이 있다.

라. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

10. 피심인은 그룹웨어의 업무용 공유폴더에서 발생하는 접속기록은 6개월 이상 저장하고 있었으나, 접속기록을 월 1회 이상 정기적으로 확인·감독한 내역을 제출하지 못한 사실이 있다.

마. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

1) 피심인의 개인정보취급자가 2017.6.21. 업무용 백업 파일(' .zip')을 업무용 공유폴더에 업로드하면서 그룹웨어에 접속 가능한 개인정보취급자의 비밀번호 및 DB접속 비밀번호를 암호화하지 않고 저장한 사실이 있으며, 개인정보취급자의 비밀번호를 2019.4.25.까지 업무용 공유폴더에 저장·공유한 사실이 있다.

2) 피심인은 업무 처리를 목적으로 엑셀 및 이미지 파일로 보관 중인 주민등록번호를 2019.5.22.까지 업무용 공유폴더에 저장·공유하였으며, 업무용 공유폴더에서 개인정보가 포함된 유출 파일(사업소득세 자료, 서비스 이용현황 세금계산서 발행, 정산 내역 회신, 호스팅 리스트 등) 중 암호화하지 않은 평문 형태의 주민등록번호 138건(55명)을 보관한 사실이 있다.

바. 처분의 사전통지 및 의견 수렴

11. 방송통신위원회는 2019. 11. 13. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 11. 27. 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.

12. 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.

13. '정보통신서비스 제공자를 위한 개인정보보호 법령 해설서'는 "정보통신망법 제23조의2제1항에 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 한다."고 해설하고 있다.

나. 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.

14. 정보통신망법 시행령 제14조의2제1항은 "정보통신서비스 제공자등은 개인정

보의 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.

15. '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)'를 하여야 한다."라고 규정하고 있다.

16. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(개인정보처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)', '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자의 경우

개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영(제4호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

17. 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.

18. 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)', '주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)', '그 밖에 암호화 기술을 이용한 보안조치(제4호)'를 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') 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다."라고 규정하고 있고, 제4조제3항은 "정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다."라고 규정하고 있다. 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있고, 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속

한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있으며 제4조제6항은 "전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다."고 규정하고 있다. 제4조제8항은 "정보통신서비스 제공자등은 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성(제1호)', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고(제2호)', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경(제3호)' 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다."라고 규정하고 있고, 제4조제9항은 "정보통신서비스 제공자등은 처리중인 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.

20. 고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

21. 고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있고, 제6조제2항은 "정보통신서비스 제공자등은 계좌번호 등 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다."라고 규정하고 있으며, 제6조제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장

매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

22. '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.

23. 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있고, 제5항에 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 업데이

트 적용 및 운영·관리하여야 한다고 해설하고 있고, 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 있으며, 제4조제6항에 대해 개인정보처리시스템에 접근하여 다운로드, 파기 또는 접근권한 설정이 가능한 개인정보취급자는 외부 인터넷망이 차단된 업무망에서 업무를 수행하여야 하며, 업무망과 외부 인터넷망은 서로의 영역에 접근할 수 없도록 물리적이나 논리적으로 망분리하여 차단하여야 한다고 해설하고 있다.

24. 고시 제4조제8항에 대해 정보통신서비스 제공자등은 개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 포함하는 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템 등에 적용하여야 하며, 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하고, 개인정보처리시스템에 권한 없는 자의 접근을 방지하기 위하여 비밀번호 등을 일정 횟수 이상 잘못 입력할 때에는 개인정보처리시스템에 접근을 제한하는 등의 보호조치를 추가적으로 적용할 수 있다고 해설하고 있고, 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.

25. 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,

26. 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 시점) 〈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.

27. 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, 비밀번호를 암호화 할때에는 국내·외 암호 연구 관련기관에서 사용 권고하는 안전한 암호 알고리듬으로 암호화하여 저장하도록 한다고 해설하며 MD5, SHA-1 등 보안강도가 낮은 것으로 판명된 암호 알고리듬을 사용하여서는 안된다(2016.9월 기준)고 해설하고 있고, 제6조제2항에 대해 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리듬(보안강도 112비

트 이상)으로 암호화하여 저장하여야하며 처리속도 등 기술발전에 따라 사용 권고 암호 알고리듬은 달라질 수 있으므로, 암호화 적용 시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인이 필요하다고 해설하고 있으며, 제6조제4항에 대해 이용자의 개인정보를 업무용 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호알고리듬이 탑재된 암호화 소프트웨어 등을 활성하고나 개인정보의 저장형태가 오피스 파일 형태일 때에는 해당 프로그램에서 제공하는 암호 설정 기능을 활용하고, MS Windows 등 운영체제에서 제공하는 암호화 기능을 활용하도록 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. 주민등록번호를 수집·이용{정보통신망법 제23조의2(주민등록번호의 사용 제한)}한 행위

28. 피심인은 본인확인기관으로 지정받은 바 없고, 법령 및 고시에서 주민등록번호의 수집·이용을 허용하는 경우에도 해당하지 않으므로 이용자의 주민등록번호를 수집·보유해서는 아니 되나, 업무 처리를 목적(개인회원의 ID 및 비밀번호 찾기, 이름 개명, 관리 ID변경, 도메인 소유권 이전, 도메인 소유자 정보변경, 네임서버 변경 등)으로 이용자의 신분증 사본 등을 수집·이용한 행위는 정보통신망법 제23조의2제1항을 위반한 것이다.

나. 개인정보의 분실·도난·유출 사실{정보통신망법 제27조의3(개인정보 유출등의 통지·신고)}을 지연 신고한 행위

29. 피심인이 개인정보 유출 피해 대상, 규모 등을 확인하고도 24시간이 경과한 이후에 방송통신위원회에 신고하고 개인정보 유출사실을 이용자에게 통지한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

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

1) (접근권한 최소부여) 피심인이 이용자의 개인정보를 처리하기 위한 업무용 공유폴더에 접속 가능한 계정의 접근권한을 사용자 및 부서별로 차등부여하지 않고, 모든 직원에게 읽기·쓰기·삭제 권한이 할당되도록 운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제1항을 위반한 것이다.

2) (접근권한 기록보관) 피심인이 개인정보처리시스템에 대하여 개인정보취급자에 대한 권한부여 및 변경 또는 말소에 대한 내역을 기록하고 최소 5년 이상 보관하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

3) (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 제15조제2항제2호, 고시 제4조제4항을 위반한 것이다.

4) (침입차단 및 탐지시스템의 설치·운영) 피심인이 2018.6.14.~2019.1.24. 기간 동안 외부 IP에서 POP3(아웃룩 메일), SSH(서버접속)을 통한 대량의 접속이 탐지되었음에도 개인정보 유출 시도를 차단하기 위해 주기적인 접속 IP 재분석을 통한 IP 차단 등 추가적인 조치하지 않은 행위 및 개인정보를 처리하고 있는

웹하드 접속 시 외부 인터넷망에서의 접근을 IP 등으로 제한하지 않고 아이디와 비밀번호만으로 접속할 수 있도록 운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

5) (망분리) 피심인이 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리를 하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제3호, 고시 제4조제6항을 위반한 것이다.

6) (비밀번호 작성규칙) 피심인이 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 사항을 포함하는 비밀번호 작성규칙을 수립하여 이를 적용·운영하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제4호, 고시 제4조제8항을 위반한 것이다.

7) (개인정보 유·노출 방지) 피심인이 그룹웨어에서 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 취하지 않아 개인정보가 다운로드(유출)되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제9항을 위반한 것이다.

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

30. 피심인이 그룹웨어의 업무용 공유폴더에 접속한 기록을 월1회 이상 정기적으로 확인·감독하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

마. 개인정보의 암호화기술 등을 이용한 보안조치{정보통신망법 제28조(개인

정보의 보호조치) 중 암호화}를 **소홀히 한 행위**

1) (비밀번호 암호화) 피심인이 그룹웨어에 접속 가능한 개인정보취급자의 비밀번호 및 DB접속 비밀번호를 암호화하지 않고 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

2) (주민등록번호 암호화) 피심인이 이용자의 주민등록번호를 안전한 암호알고리듬으로 암호화하지 않고 평문으로 업무용 공유폴더에 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제2·4호, 고시 제6조제2·4항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	주민등록번호	§23의2①		법적 근거없이 이용자의 주민등록번호를 수집·이용한 행위
	지연통지신고	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근통제	§28①2호	§15②1호	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 아니한 행위(고시§4①)
	접근통제	§28①2호	§15②1호	개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근통제	§28①2호	§15②2호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	접근통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치·운영하지 아니한 행위(고시§4⑤)
	접근통제	§28①2호	§15②3호	개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리 적용하지 아니한 행위(고시§4⑥)
	접근통제	§28①2호	§15②4호	개인정보취급자의 비밀번호 작성규칙을 수립·운영하지 않은 행위(고시§4⑧)
	접근통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
	접속	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	기록			작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④1호	비밀번호를 안전한 암호알고리듬으로 일방향 암호화하여 저장하지 아니한 행위(고시§6①)
	암호화	§28①4호	§15④2·4호	이용자의 주민등록번호 등에 대해 안전한 알고리듬으로 암호화 하지 않고 평문으로 파일에 저장한 행위(고시§6②·④)

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

소 5년간 보관할 것 3)개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것 4)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 5)개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것 6)개인정보처리시스템에 접근할 수 있는 개인정보취급자의 비밀번호는 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성, 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고, 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하는 사항 등을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용할 것 7)취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것 8)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리할 것 9)비밀번호는 복호화되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것 10)이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리듬으로 암호화하여 저장할 것 11)이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화할 것

라. 피심인은 가항부터 다항까지의 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) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ① 법적 근거없이 이용자의 주민등록번호를 수집·이용한 행위 ② 개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위 ③ 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여하지 않은 행위 ④ 개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 않은 행위 ⑤ 외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 않은 행위 ⑥ 개인정보처리시스템에 침입차단 및 침입탐지시스템 설치·운영을 소홀히 한 행위 ⑦ 개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리 적용하지 않은 행위 ⑧ 개인정보취급자의 비밀번호 작성규칙을 수립·운영하지 않은 행위 ⑨ 홈페이지 등에 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등 조치를 취하지 않은 행위 ⑩ 개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 않은 행위 ⑪ 비밀번호를 안전한 암호알고리즘으로 일방향 암호화하여 저장하지 않은 행위 ⑫ 이용자의 주민등록번호 등에 대해 안전한 알고리즘으로 암호화 하지 않고 평문으로 저장한 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

31. 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

32. 피심인은 정보통신망법 제64조의3제1항제6호에 따라 이용자의 개인정보가

분실·유출된 경우로서 개인정보 보호조치(제28조제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할 수 있다.

33. 피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정 기준과 산정절차) 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(이하 '과징금 부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

34. 피심인의 정보통신망법 제28조제1항 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.

나. 기준금액

1) 고의 · 중과실 여부

35. 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.

36. 이에 따를 때 정보통신망법 제28조제1항 기술적·관리적 보호조치 중 접근통제를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고

판단한다.

2) 중대성의 판단

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

38. 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.

39. 이에 따라 피심인이 위반행위로 직접적인 이득은 취하지 않았다는 점을 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

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

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2016년	2017년	2018년	평균
관련 매출액				

※ 자료출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

<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

41. 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내 '단기 위반행위'에 해당하므로 기준금액을 유지하고,

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

라. 추가적 가중 및 감경

43. 과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

44. 이에 따를 때 피심인이 조사에 성실히 협조한 점을 고려하여 필수적 가중·감경을 거친 금액의 100분의 10에 해당하는 원을 감경한다.

2. 과징금의 결정

45. 피심인의 정보통신망법 제28조(개인정보의 보호조치) 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 금액인 원이나, 최종 과징금 산출액이 1억원 이상에 해당하여 백만원 미만을 절사한 494,000,000원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
천원	필수적 가중 없음 필수적 감경 (50%, 천원)	추가적 가중 없음 추가적 감경 (10%, 천원)	**49,400만원**
	→ 천원	→ 천원	

* '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

46. 피심인의 정보통신망법 제23조의2(주민등록번호의 사용 제한)제1항, 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제2호·제2호의3·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

47. 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

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.

48. 이에 따라 피심인의 정보통신망법 제27조의3제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 경우에 해당하므로 기준금액의 30%인 300만원을 가중하고, 피심인의 정보통신망법 제28조제1항 위반행위에 대해 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하므로 기준

금액의 50%인 500만원을 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.

49. 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
§23의2①	1,000만원	없음	없음	**1,000만원**
§27의3①	1,000만원	300만원	없음	**1,300만원**
§28①2·3·4호	1,000만원	500만원	500만원	**1,000만원**
계				**3,300만원**

다. 최종 과태료

50. 이에 따라 피심인의 정보통신망법 제23조의2제1항, 제27조의3제1항, 제28조제1항 위반행위에 대해 33,000,000원의 과태료를 부과한다.

Ⅶ. 결론

51. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

52. 피심인은 이 시정명령 및 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할

수 있다.

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

54. 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 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)