방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 38 - 174호

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 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 제한

하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것

라. 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

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

바. 비밀번호는 복호화되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것

2. 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.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 8,000,000원

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 취업정보 제공 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 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 개인정

보 취급·운영 실태를 조사 하였고, 피심인에 대한 현장조사(2019. 10. 24.~10. 25., 2020. 2. 18.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 취업정보 제공 사이트를 운영하면서 2019. 12. 31. 기준 아래와 같이 이용자의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
유효회원	이름, 생년월일, 성별, 아이디, 비밀번호, 이메일, 휴대전화번호, 주소, 일반전화번호 등		건
휴면회원	상동		건
총계			건

나. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

- 2019. 10. 22. 14:10 자칭 '해킹크루 weus'라는 해커로부터 1억원 상당의 비트코인을 요구하는 협박 메일에 첨부된 개인회원 DB(100건) 및 관리자정보 DB(198건) 엑셀파일을 받고 개인정보 유출 사실 인지
- 2019. 10. 22. 17:30 한국인터넷진흥원에 유출신고 및 침해사고 신고, 경찰청 사이버수사대에 수사 의뢰
- 2019.10.23. 13:30 개인회원 대상 이메일 통지 및 홈페이지 팝업 공지

2) 개인정보 유출 규모

4. 피심인이 취업정보 제공 사이트를 운영하면서 수집한 회원의 개인정보 9,462건이 훼손(삭제, 비밀번호 변경) 및 유출되었으나 로그에서 발생된 데이터를 별도로 기록하고 있지 않아 정확한 유출규모는 알 수 없으며, 해커가 보내온 메일에 첨부된 개인정보 건수는 아래와 같다.

< 피심인의 개인정보 유출현황 >

구분	항목	건수
개인회원	이름, 성별, ID, 비밀번호(암호화), 생년월일, 이메일주소, 전화번호, 이동전화번호, 주소 등	100건
관리자 정보	ID, 비밀번호(평문),이름, 이메일주소, 이동전화번호 등	198건
총계		298건

3) 유출 경로

- 2019. 4. 1. 해커는 홈페이지의 다운로드 취약점을 악용하여 홈페이지 내 웹소스, DB 정보가 포함된 파일을 다운로드하였고, 2019. 4. 4. 웹쉘 업로드 및 '19. 10. 21. 실행을 통한 회원정보(9,462건) 유출 및 삭제함
- 2019. 4. 1. 11:02 ~ '19. 4. 4. 09:58 다운로드 취약점을 악용하여 ASP 소스 파일 등 146회 다운로드하였으며, 소스 파일 중 업로드 취약점이 존재하는 file .asp 파일 확인
- 2019. 4. 4. 10:00 ~ 15:11 file .asp에 존재하는 업로드 취약점을 악용하여 웹쉘 55회 업로드 시도하고 zip .asp 웹쉘 업로드 성공
- 2019. 4. 4. 16:15 zip .asp 웹쉘을 악용하여 job .asp 추가 웹쉘 업로드 성공
- 2019. 10. 21. 16:18 ~ 17:49 웹쉘 2종을 66회 실행하여 DB 내 회원정보 삭제 및 이미지 폴더 삭제 추정

- 2019. 10. 22. 16:33 ~ 18:25 웹쉘 2종을 38회 실행하여 DB 내 Password 변경 추정

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

1) 피심인은 부터 등록된 개인정보취급자 198명에 대한 퇴사, 인사이동 등이 있었음에도 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않았으며, 현장조사 당시 사용하지 않는 개인정보 취급자 권한 193명에 대해 권한을 말소한 사실이 있다.

2) 피심인은 개인정보취급자에 대한 권한 부여, 변경 또는 말소에 대한 내역의 기록을 5년 이상 보관하지 않은 사실이 있다.

3) 피심인은 2016. 3. 28.부터 2019. 10. 25.까지 웹 방화벽에서 HTTP 비정상 요청, 웹쉘 업로드, SQL 인젝션 등 웹 공격에 대해 탐지·차단하고 있었으나, 차단·탐지 이력을 재분석하여 공격 시도 IP에 대하여 차단 IP로 등록하거나, 업로드 경로의 이상 유무를 확인하는 등 추가적인 조치를 수행하지 않은 사실이 있다.

4) 피심인은 개인회원 비밀번호에 대해서는 '8~20자 영문, 숫자, 특수문자를 혼용 사용'토록 비밀번호 작성규칙을 수립·적용하고 있었으나, 개인정보취급자와 기업회원에 대해서는 별도의 비밀번호 작성규칙을 수립·적용하지 않은 사실이 있다.

5) 피심인은 부터 2019. 10. 25까지 운영 중인 홈페이지 내 다운로드 취약점과 업로드 취약점이 존재하여, 해커가 2019. 4. 1.부터 2019. 4. 4까지 웹쉘 2종을 업로드하여 2019. 10. 21. 웹 쉘을 통해 개인정보 9,462건을 훼손(삭제, 패스워드 변경) 및 유출한 사실이 있다.

나. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

5. 피심인은 개인정보취급자와 기업회원의 비밀번호를 암호화하지 않고 평문으로 DB에 저장한 사실이 있다.

다. 처분의 사전통지 및 의견 수렴

6. 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. 13. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 이용한 보안조치(제4호)'를 하여야 한다."라고 규정하고 있다.

7. 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)', '비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영(제4호)', 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'를 하여야 한다."라고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)'을 하여

야 한다."라고 규정하고 있다.

8. 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 있고, 제3항은 "정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다."라고 규정하고 있으며, 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 있고, 제8항은 " 정보통신서비스 제공자등은 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성(제1호)'하는 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다."라고 규정하고 있으며, 제9항은 "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.

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

10. '고시 해설서'는 고시 제4조제2항에 대해 정보통신서비스 제공자등은 불완전한 접근권한의 변경 또는 말소 조치로 인하여 정당한 권한이 없는 자가 개인정보처리시스템에 접근할 수 없도록 하여야 한다고 해설하고 있고,

제3항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 5년간 보관하여야 하며, 관리대장 등에는 신청자 정보, 신청 및 적용일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하도록 한다고 해설하고 있으며, 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), 웹 방화벽, 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 하며 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, 제8항에 대해 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문, 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 있으며, 제9항에 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 해설하

고 있다.

11. 고시 제6조제1항에 대해 정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조 되지 않도록 개인정보처리시스템, 업무용컴퓨터, 보조저장매체 등에 일방향 암호화(해쉬함수 적용)하여 저장하여야 하며 무작위 대입공격(Brute Force), 레인보우 테이블 공격 등을 이용한 비밀번호복호화에 대응하기 위하여 난수추가(salting) 등의 조치를 하여야 하며 국내·외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호 알고리듬으로 암호화하여 저장하고, 보안강도가 낮은 것으로 판명된 암호 알고리듬(MD5, SHA-1 등)을 사용해서는 안된다고 해설하고 있다.

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

1) (접근권한 변경·말소) 피심인이 부터 등록된 개인정보취급자 198명에 대한 퇴사, 인사이동 등이 있었음에도 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제2항을 위반한 것이다.

2) (접근권한 기록보관) 피심인이 개인정보취급자에 대한 권한 부여, 변경 또는 말소에 대한 내역의 기록을 5년 이상 보관하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

3) (침입차단 및 탐지시스템의 설치·운영) 피심인이 2016. 3. 28.부터 2019. 10. 25.까지 웹 방화벽에서 HTTP 비정상 요청, 웹쉘 업로드, SQL 인젝션 등 웹 공격에 대해 탐지·차단하고 있었으나, 차단·탐지 이력을 재분석하여 공격 시도 IP에 대하여 차단 IP로 등록하거나, 업로드 경로의 이상 유무를 확인하는 등 추가적인 조치를 수행하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

4) (비밀번호 작성규칙) 피심인이 개인정보취급자와 기업회원에 대해서는 별도의 비밀번호 작성규칙을 수립·적용하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제4호, 고시 제4조제8항을 위반한 것이다.

5) (개인정보 유·노출 방지) 피심인이 부터 2019. 10. 25까지 운영 중인 홈페이지 내 특정 파일을 다운로드 할 때 사용하는 ASP 페이지의 다운로드 취약점과 자격증, 졸업증명서 등 입사지원 시에 필요한 첨부파일을 관리하는 페이지의 업로드 취약점이 존재하여, 해커에 의해 2019. 4. 1.부터 2019. 4. 4까지 웹쉘 2종이 업로드 되어 2019. 10. 21. 웹 쉘을 통해 개인정보 9,462건이 훼손(삭제, 패스워드 변경) 및 유출되게 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

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

12. 피심인이 개인회원의 비밀번호는 안전한 일방향 암호 알고리듬(SHA256, XecureDB 암호화솔루션)으로 암호화 후 BASE64로 인코딩하여 DB에 저장하고 있었으나, 개인정보취급자와 기업회원의 비밀번호는 암호화하지 않고 평문으로 DB에 저장한 행위는, 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	인사이동 발생 시 지체 없이 개인정보처리시스템 접근권한을 변경 또는 말소하지 아니한 행위(고시§4②)
	접근 통제	§28①2호	§15②1호	접근권한의 부여·변경·말소에 대한 기록을 5년 이상 보관하지 아니한 행위(고시§4③)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 운영하지 아니한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②4호	개인정보취급자에 대한 비밀번호 작성규칙을 수립·이행하지 아니한 행위(고시§4⑧)
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 유·노출되지 아니하도록 컴퓨터 등에 조치하지 아니한 행위(고시§4⑨)
	암호화	§28①4호	§15④1호	개인정보 취급자의 비밀번호를 일방향 암호화하여 저장하지 아니한 행위(고시§6①)

Ⅳ. 시정조치 명령

1. 시정명령

13. 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 시

도를 탐지하는 기능을 포함한 시스템을 설치·운영할 것 4)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 5)취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취할 것 6)비밀번호는 복호화 되지 아니하도록 안전한 암호알고리즘을 이용하여 일방향 암호화하여 저장할 것

2. 시정명령 이행결과의 보고

14. 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

15. 피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 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

16. 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 적용한다.

〈 위반 횟수별 과태료 금액 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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.

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

18. 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
§28①2·4호	1,000만원	300만원	500만원	**800만원**
계				**800만원**

다. 최종 과태료

19. 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 8,000,000원의 과태료를 부과한다.

Ⅵ. 결론

20. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

21. 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.

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

23. 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)