방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 35 - 385호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2018. 7. 11.

주 문

1. 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.

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. 개인정보관리책임자 또는 개인정보취급자에 대한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관할 것

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

다. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

라. 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장할 것

마. 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 제1항부터 제3항까지의 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.

5. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 35,000,000원

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

피심인은 영리를 목적으로 홈페이지( )를 통해 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법' 이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈참고 1〉 피심인의 일반현황

대표이사	설립일자	자본금	주요서비스	종업원 수

〈참고 2〉 피심인의 최근 3년간 매출액 현황

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

경찰청이 ' ' 해커를 추가 조사하는 과정에서 피심인의 개인정보가 유출되었다는 내용을 방송통신위원회에 알려옴('18.1.24.)에 따라, 방송통신위원회는 피심인을 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2018.3.15.~2018.3.16.) 결과, 다음과 같은

사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘ 안내’ 서비스를 운영하면서 2018. 3. 15. 기준으로 4,428건의 회원정보를 보유하고 있다.

〈참고 3〉 피심인의 개인정보 수집 현황

구 분	항 목	수집기간	건수
홈사이트 회원	[필수] 아이디, 이름, 비밀번호, 생년월일, 성별, 주소, 휴대전화번호, 이메일 [선택] 직업, 회사명, 회사주소, 최종학력, 결혼기념일 등	'09.9.14. ~	4,428건

나. 개인정보 유출 규모 및 경로

(1) 개인정보 유출규모

피심인이 ‘ 안내’서비스를 운영하면서 수집한 회원의 개인정보 4,075건이 유출되었다.

〈참고 4〉 피심인의 개인정보 유출 현황

구 분	유 출 항 목	건 수
홈페이지 회원	아이디, 성명, 비밀번호, 생년월일, 이메일, 집주소, 휴대전화번호, 집전화번호	4,075건

(2) 유출 경로

2016.10.28. 피심인의 홈페이지에 접속 장애가 발생되어 피심인은 이를 처리

하는 과정에서 악성코드를 삭제하고 재부팅하여 복구하였으나, 접속장애 발생 전에 삭제했던 악성코드에 감염되어 DB 개인정보 4,075건이 유출된 것으로 추정된다.

(3) 유출 신고

피심인은 2017.7.11. 숙박앱 ' ' 를 해킹한 해커 일당으로부터 압수한 추가적인 개인정보 파일과 관련된 경찰청 조사과정에서 유출 사고를 인지하였다.

피심인은 2017.7월말. 개인정보 유출사실을 홈페이지에 공지하였으며, 2017.7.28. 유출 대상자에게 1차로 이메일 개별 통지(발송 3,901, 실패 588)하고, 2017.8.1. ~ 14. 유출 대상자에게 2차로 문자메시지를 개별 통지(발송 664, 실패 110)하였다.

피심인은 「개인보보 보호법」 적용사업자로 판단하여 유출이 1만건 이상의 경우에만 신고해야 하는 것으로 알고 신고하지 않았으나, 정보통신망법이 적용되는 사업자임을 알고 2018.3.16. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 유출을 신고하였다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

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

피심인은 개인정보 유출사실을 인지한 때(2017.7.11.)로부터 17일이 경과하여 이용자에게 통보하고, 현장조사(2018.3.15.) 시까지 개인정보보호 포털(i-privacy.kr, KISA)에 신고하지 않은 사실이 있다.

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

1) **(접근권한 기록보관)** 피심인은 개인정보처리시스템(DB, 관리자페이지)에 대한 접근권한 부여, 변경 또는 말소에 내역을 기록하고 보관한 사실이 없다.

2) **(안전한 인증수단)** 피심인은 개인정보취급자가 현재 개인정보처리시스템(관리자페이지)에 접속할 때, 접근 가능한 IP에서 VPN을 통해 접속하도록 설정하여 운영하고 있으나, 2017.7.11. 개인정보 유출 인지 이전에는 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 외부에서 접속이 가능하도록 한 사실이 있다.

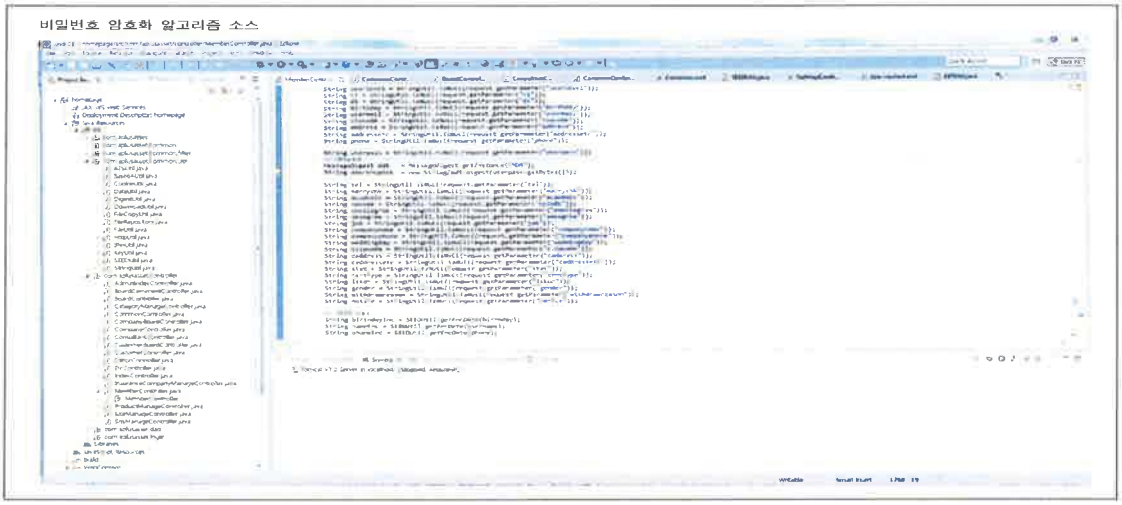
다. 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 DB에 접속한 일시, 처리내역 등 접속기록을 보존·관리하지 아니하였고, 접속시간·성명·접속IP주소 등 관리자페이지 접속한 기록은 6개월 이상 보존·관리하고 있으나, 수행업무내용은 보존·관리하지 아니하였으며, DB 및 관리자페이지 접속기록을 월1회 이상 정기적으로 확인·감독한 사실이 없다.

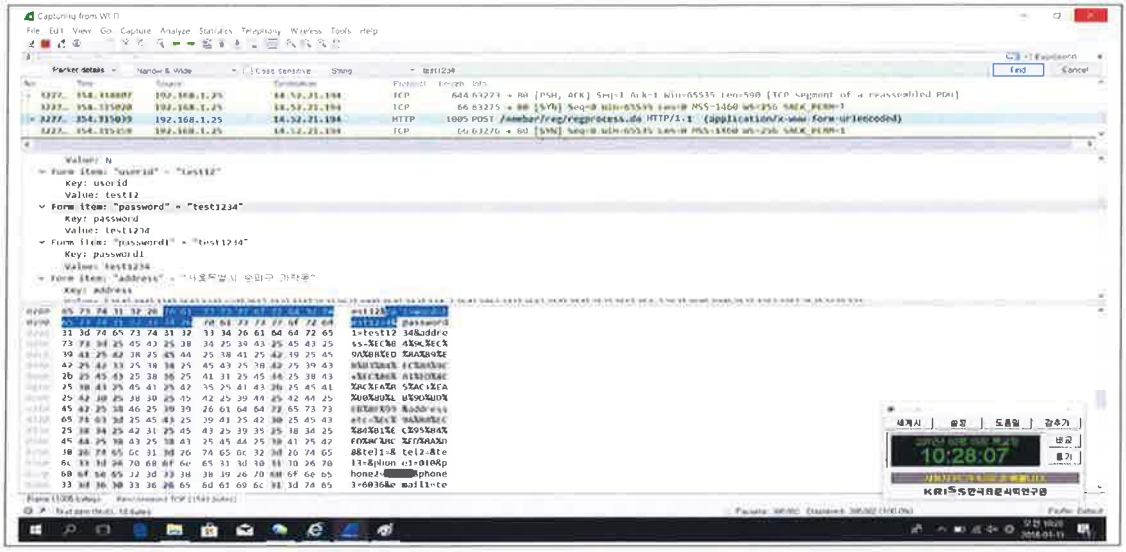
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-05-2018 13:44:17
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-05-2018 13:41:33
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-05-2018 11:15:00
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-04-2018 17:24:38
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-04-2018 10:30:28
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-04-2018 08:54:07
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-03-2018 17:21:01
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-02-2018 17:30:07
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-02-2018 15:21:24
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-02-2018 14:16:43
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	01-02-2018 10:20:56
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-29-2017 13:40:16
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-29-2017 10:02:59
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-28-2017 11:29:38
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-27-2017 15:07:12
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-27-2017 13:20:33
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-22-2017 11:48:38
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-22-2017 09:54:39
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-21-2017 14:55:52
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-21-2017 09:35:38
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-20-2017 10:30:33
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-19-2017 16:53:48
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-18-2017 16:02:33
관리부문	정보시스템팀	정보개발파트	정보개발파트	86350000	99995000	홈페이지관리자	192.168.102.32	12-18-2017 10:22:56

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

1) **(비밀번호 암호화)** 피심인은 홈페이지 이용자의 비밀번호를 개인정보처리시스템에 안전하지 않은 MD5[1]방식으로 암호화하여 저장한 사실이 있다.



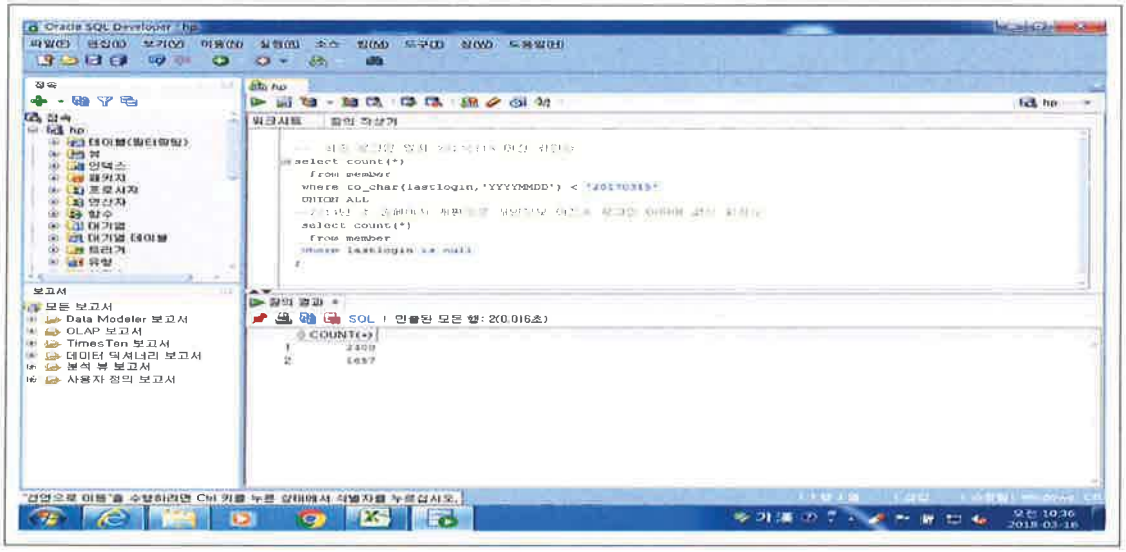
2) **(전송구간 암호화)** 피심인은 이용자가 정보통신망을 통해 홈페이지 회원가입 및 로그인 시 아이디, 이름, 전화번호 등의 개인정보를 암호화하지 않고 송·수신 되도록 한 사실이 있다.



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

1) MD5 : 'Message-Digest algorithm 5'의 약자로 128비트 길이의 해시값을 출력하는 알고리즘, 보안강도 80비트 미만으로 현재 역방향에 대한 어느정도 추론이 가능하여 비밀번호와 같이 기밀성이 보장되어야 하는 곳에는 쓰지 않는다.

피심인은 운영중인 홈페이지를 통해 이름, 생년월일, 전화번호, 이메일 등을 수집하여 2018.3.15. 현재 4,428명의 이용자 정보를 피심인의 개인정보처리시스템 내 회원DB에 저장·관리하고 있다. 그러나 이 가운데 1년 동안 서비스를 이용하지 아니한 이용자 4,057명의 개인정보에 대해서는 이를 파기하지 않았으며, 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.



바. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 4. 26. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 5. 10. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 " 유출등 "이라 한다) 사실을 안 때에는 지체 없이 '유

출등이 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.

정보통신망법 시행령 제14조의2제1항은 "정보통신서비스 제공자등은 개인정보의 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." 라고 규정하고 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)'를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)'의 조치를 하여야 한다." 라고 규정하고 있고, 제3항은 "접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)'의 조치를 하여야 한다." 라고 규정하고 있으며, 제4항은 "개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)', '정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버

구축 등의 조치(제3호)' 조치를 하여야 한다." 라고 규정하고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시'라 한다) 제4조제3항은 "개인정보처리시스템에 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다." 고 규정하고 있고, 제4조제4항은 "개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다." 라고 규정하고 있다.

고시 제5조제1항은 "개인정보취급자가 개인정보 처리시스템에 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.

고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다." 라고 규정하고 있고, 제6조제3항은 "정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다." 라고 규정하고 있다.

다. 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.

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.

라. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자 등이 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. 개인정보의 분실·도난·유출 사실{정보통신망법 제27조의3(개인정보 유출 등의 통지·신고)}**을 지연 신고한 행위**

정보통신망법 제27조의3제1항의 '지체 없이'에 대해서 정보통신망법에 별도로 규정된 정의는 없으나, 관련 판례에서는 '합리적인 이유 및 근거가 없는 한 즉시'로 해석하고 있다.

따라서 피심인이 개인정보의 유출 사실을 안 때(2017.7.11.)로부터 17일이 경과한 2017.7.27. 개인정보가 유출된 이용자 4,428명에게 이메일과 문자메시지로 개별 통보하고, 248일이 경과한 2018.03.16.에 개인정보보호 종합포털(privacy.go.kr)에 신고한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

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

1) (접근권한 기록보관) 고시 제4조제3항의 입법 목적은 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 적용 일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하도록 한다는 것이다.

피심인이 개인정보처리시스템에 대한 권한부여, 변경 또는 말소에 대한 내역을 최소 5년간 보관하지 않은 행위는 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

2) (안전한 인증수단) 고시 제4조제4항의 입법 목적은 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 필요하다는 것이다.

피심인이 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 별도의 안전한 인증수단(ex. 보안토큰, 휴대폰 인증 등) 없이 아이디와 비밀번호만으로 접속이 가능하게 한 행위는 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

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

고시 제5조제1항의 입법 목적은 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), 접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)), 접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), 수행업무(개인정보처리시스템에서 개인정보취급자가 처리(개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위)한 내용을 알 수 있는 정보) 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다는 것이다.

피심인이 개인정보취급자의 DB 및 관리자페이지 등 개인정보처리시스템에

접속한 처리일시, 처리내역 등 접속기록을 최소 6개월간 보존·관리하지 아니하고, 개인정보처리시스템의 접속기록을 월1회 이상 정기적으로 확인·감독하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

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

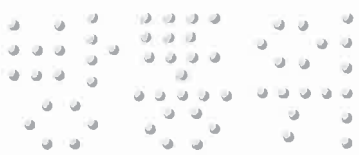
1) (비밀번호 암호화) 고시 제6조제1항의 입법 목적은 개인정보취급자 및 이용자의 비밀번호가 노출 또는 위·변조되지 않도록 일방향 함수(해쉬함수, 128비트 보안강도 권고)를 이용하여 저장하여야 한다는 것이다.

피심인이 이용자의 비밀번호를 개인정보처리시스템(회원DB)에 저장할 때 개인정보가 노출 또는 위·변조되지 않도록 일방향 암호화알고리즘으로 암호화(해쉬함수, 128비트 보안강도 권고) 하지 않고 안전하지 않은 암호알고리즘인 MD5를 이용하여 이용자의 비밀번호를 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제1호, 고시 제6조제1항을 위반한 것이다.

2) (전송구간 암호화) 고시 제6조제3항의 입법 목적은 이용자의 성명, 연락처 등의 개인정보와 인증정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 한다는 것이다.

피심인이 이용자의 PC에서 홈페이지 회원가입 및 로그인 시 개인정보처리시스템으로 개인정보를 전송하는 구간에 대하여 암호화하지 않은 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령 제15조제4항제3호, 고시 제6조제3항을 위반한 것이다.

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



피심인이 정보통신서비스를 1년의 기간 동안 이용하지 아니한 이용자의 개인정보 4,057건을 파기하거나 다른 이용자와 별도로 저장·관리하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

〈참고 5〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	지연 신고	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 알리고 신고한 행위
	접근 통제	§28①2호	§15②1호	개인정보취급자에 대한 권한부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근 통제	§28①2호	§15②2호	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 감독하지 않고, 최소 6개월 이상 접속기록을 보존하지 아니한 행위(고시§5①)
	암호화	§28①4호	§15④1호	이용자의 비밀번호를 안전하지 않은 암호화 방법으로 저장한 행위(고시§6①)
	암호화	§28①4호	§15④3호	이용자의 개인정보 및 인증정보를 송·수신 할 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

Ⅳ. 시정조치 명령

1. 시정명령

가. 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 이용자에

게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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) 개인정보관리책임자 또는 개인정보취급자에 대한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

4) 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장할 것

5) 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.

2. 시정명령 이행결과의 보고

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. 과태료 부과

피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항 위반에 대한 과태료는 같은 법 제76조제1항제2호의3·제3호·제4호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '과태료 부과 등 처리지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과 등 처리지침 제7조는 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.

〈참고 6〉 위반 횟수별 과태료 금액

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조 제1항제4호	1,000	2,000	3,000

나. 과태료의 가중

과태료 부과 등 처리지침 제9조는 ▲위반행위가 2개 이상인 경우, ▲위반행위가 2개 이상에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기·정도, 사회·경제적 파급 효과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, 과태료 부과 등 처리지침 제7조에 따른 과태료 금액

을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위가 2개 이상인 경우에 해당하므로 기준 금액의 50%를 가중한다.

〈참고 7〉 과태료 산출내역

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

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제27조의3제1항, 제28조제1항, 제29조제2항 위반행위에 대해 3,500만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제2호의3·제3호·제4호에 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.

위 원 장 이 효 성 (인)

부위원장 허 욱 (인)

위 원 김 석 진 (인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)