방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020 - 23 - 112호

안 건 명 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2020. 4. 29.

주 문

1. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 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. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 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. 이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리듬으로 암호화하여 저장할 것

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

3. 피심인은 제1항부터 제2항까지의 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.

4. 피심인에 대하여 다음과 같이 과태료 및 과징금을 부과한다.

가. 과 징 금 : 27,200,000원

나. 과 태 료 : 13,000,000원

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 서비스 등을 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 : 천원)

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 개인정보보호 포털에 유출신고 한 사업자에 대하여 정보통신망법 위반 여부에 대한 피심인의 개인정보 취급·운영 사실을 조사(2019.5.2.~5.3., 5.7.~5.8., 5.13.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3 피심인은 서비스 제공을 위한 홈페이지( )를 부터 운영하면서, 2019. 5. 3. 현재 아래와 같이 이용자의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구분	항목	수집일	건수
이용자정보 (유효회원)	**[개인회원]** (필수) 주소, 이메일 주소 (선택) 휴대폰번호, 계좌정보(은행명, 계좌번호, 계좌주명), 주민등록번호(수입 지급 필수)		
	[사업자 회원] (필수) 대표자명, 주소, 이메일 주소 (선택) 휴대폰 번호, 계좌정보(은행명, 계좌번호, 계좌주명), 대표 전화번호, 팩스번호		
(휴면회원)	**[개인 회원]** 아이디, 이름, 메일주소, 휴대폰번호, 주소, 계좌정보, 주민등록번호 **[사업자 회원]** 아이디, 이메일주소, 휴대폰 번호, 사업자 정보, 계좌 정보		
계			

나. 서비스 제공을 위한 신규 재무관리시스템 개발과정

4 피심인은 매년 4월 수입 지급·전환액에 대한 원천징수영수증을 발급하고 있으며, 지급받은 수입이 일정금액을 초과하는 이용자들에게 원천징수영수증을 메일로 발송하고 있다.

5 피심인은 원천징수영수증을 PDF파일로 생성하여 메일로 발송하는 기능을 포함한 재무관리시스템을 Flex언어*로 개발하여 2010. 6월부터 2018. 5월까지 사용하였다.

* Adobe사에서 제공하는 프로그래밍 언어

6 피심인은 Adobe사의 Flex언어에 대한 기술지원 중단('20년 말)이 예정됨에 따라 재무관리시스템에 보안취약점 등 문제가 발생할 수 있어 2016. 7. 26. 해당 시스템을 Javascript 언어*로 개발하기로 하였다.

* 웹에서 제어가 가능한 프로그래밍 언어

< 업무관리프로그램에 신규 재무관리시스템(개발 계획을 등록 >

7 피심인은 신규 재무관리시스템( )을 개발하면서 원천징수영수증을 PDF파일로 생성하여 메일로 발송하는 소스코드를 잘못 개발*하였고 잘못된 소스코드를 2017. 3. 10. 시스템에 반영하였다.

* DB에서 불러온 개인정보를 웹문서(xml형식)로 저장하여 원천징수영수증(PDF파일)을 생성하고 메일을 발송한 후 웹문서(xml형식)로 저장된 개인정보는 삭제해야 되나, 삭제하지 않고 다른 개인정보를 기존 웹문서(xml형식)에 누적하여 원천징수영수증을 생성하도록 개발됨

< 개인정보 유출의 원인이 된 소스코드 >

8 피심인은 2017. 3. 16. 신규 재무관리시스템( )에서 원천징수영수증을 PDF파일로 생성하여 메일로 발송하는 기능에 대해 개발자에게 메일로 안내한 것 외에 실제 테스트를 진행하지는 않았다.

< 원천징수영수증 발송 안내(메일) >

g 피심인은 신규 재무관리시스템 에 대해 관련 업무담당자를 대상으로 2017. 5. 10.부터 5. 21.까지 실제 운영환경과 동일하게 현업 테스트를 해줄 것을 요청하였으나, 특이사항은 회신되지 않았고 2017. 5. 22. 실제업무에 사용하도록 배포하였다.

< 관련 업무담당자 대상 테스트요청 메일 >

< 신규 재무관리시스템 실제 업무사용 배포 >

10 2018년 원천징수영수증 발급의 경우 업무담당자의 요청에 따라 Javascript 언어로 신규 개발된 재무관리시스템 을 사용하지 않고, 기존 Flex 언어로 개발된 시스템을 사용하여 2018. 5. 2., 5. 4. 두 차례에 걸쳐 원천징수영수증을 발급하였다.

11 피심인은 2019. 2. 28.까지 신규 재무관리시스템 에 반영된 소스코드가 저장된 파일을 수차례 수정*하였으나, 개인정보 유출에 직접적인 영향이 된 소스코드의 경우 문제점을 발견하지 못하였다.

* 대부분 국세청 원천세지급명세서 신고와 관련된 사항으로 국세청 지침 등 변경사항을 반영한 작업을 수행

다. 신규 재무관리시스템 을 통한 원천징수영수증 발송

12 피심인은 2019. 4. 29. 21:00부터 4. 30. 07:33까지 원천징수영수증 발급 대상자 2,334명을 선정(2018. 1 ~ 8월 기간 소득합이 166,666원 초과하는 이용자)하여 소스코드에 문제가 있는 신규 재무관리시스템 의 원천징수영수증 생성 및 메일 발송기능을 통해 이용자들에게 원천징수영수증을 메일로 발송하였다.

※ 이용자가 열람한 메일에 첨부된 원천징수영수증 총 1,940,768건에는 다른 이용자 2,331명의 개인정보가 포함되어 있었음

< 원천징수영수증 생성·발송 >

라. 개인정보 유출 경위

1) 개인정보 유출 경과 및 대응

일시		대응 내용
4.29.	21:00	이용자 대상 원천징수영수증 포함한 메일 6,758건 발송
4.30.	03:06	원천징수영수증 수신자로부터 개인정보 유출 전화문의 접수 (개인정보 유출 사실 인지)
	11:02	메일관리시스템의 소급관리 Tool 을 통해 이용자가 열람하지 않은 메일(3,152건) 삭제 진행
	11:45	방송통신위원회 개인정보보호 포털(i-privacy.kr)에 유출 신고
	13:14	메일 삭제스크립트를 통해 이용자가 열람한 메일(3,420건)에 대해 삭제 진행
	13:21	개인정보 유출 원인에 대한 조치 완료 - 원천징수영수증 첨부파일(PDF)을 생성하는 프로그램의 소스코드 수정 완료
	16:12	유출통지(1차) 메일 발송 시작(2,183명에게 발송 완료)
	18:21	유출통지(2차) 메일 발송 시작(탈퇴회원 39명에 대해 발송 완료)
	18:42	웹사이트 개인정보 유출 공지
	20:21	타사 메일을 이용하는 이용자 18명에 대하여 메일 삭제 요청 및 전화를 받지 않는 4명에 대하여 SMS 안내
5. 1.	19:23	유출통지(3차) 메일 발송 시작(추가 확인된 112명에 대해 발송 완료)

2) 개인정보 유출 규모

13 피심인이 원천징수영수증 발급대상자 2,334*명에게 신규 재무관리시스템 의 원천징수영수증 생성 및 메일 발송기능을 통해 총 6,758건의 메일을 발송하는 과정에서 메일에 로그인한 이용자가 열람한 3,685건(타사 메일로 발송된 61건 포함)에는 총 1,940,768개의 원천징수영수증, 중복제거 시 2,331명의 개인정보가 유출되었다.

* 전년도 수익의 합이 166,666원을 초과하는 대상자로서 2018. 1월~8월 기간 기타소득 원천징수영수증 발급대상자

< 피심인의 개인정보 유출현황 >

구분	유출항목	유출시기	건수	중복제거**
이용자정보	이름, 주소, 주민등록번호*, 지급액	'19. 4. 29. ~ 4. 30	1,940,768개의 원천징수영수증	**2,331명**

* 「소득세법」 제21조(기타소득) 및 같은 법 제164조에 따른 주민등록번호 수집
** 유출된 개인정보 중 이름 기준으로 중복제거

3) 유출 경로

14 피심인은 2016. 7. 26. 신규 재무관리시스템 을 개발하면서 소스코드*를 잘못 개발한 상태로 2017. 3. 10. 시스템에 반영하고, 2019. 4. 29 ~ 4. 30 까지 원천징수영수증 발급 대상자에게 신규 재무관리시스템 의 원천징수영수증 생성 및 메일 발송기능을 통하여 메일을 보내는 과정에서 개인정보가 유출되었다.

* DB에서 불러온 개인정보를 메일로 발송한 후 삭제되어야 되나, 삭제되지 않고 다른 개인정보를 누적하여 원천징수영수증을 생성하도록 개발됨

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 보안메일 열람 시 이용자의 주민등록번호를 사용한 행위

15 피심인은 이용자에게 원천징수영수증을 PDF파일로 생성하여 메일로 발송하면서, 이용자의 주민등록번호 뒤 7자리를 비밀번호로 사용하여 원천징수영수증 PDF파일을 포함하고 있는 보안메일(HTML파일)을 열어볼 수 있도록 조치한 사실이 있다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위

16 피심인이 운영하는 신규 재무관리시스템 에 관리자 권한(개인정보취급자 그룹의 권한 변경, 개인정보 파일 다운로드 가능)으로 접속한 상태에서도 외부인터넷망이 동시 접속되도록 운영한 사실이 있다.

17 피심인은 신규 재무관리시스템 을 개발한 후 실제 운영환경과 동일한 테스트를 수행하지 않았고, 개인정보 유출에 영향을 미칠 수 있는 위험요소를 분석하여 에러·오류상황이 불충분하게 처리되지 않도록 구성하는 등 보안대책을 마련한 사실이 없으며 취급중인 개인정보가 시스템의 메일 발송기능을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 기술적·관리적 보호조치를 하지 않은 사실이 있다.

다. 개인정보의 암호화를 소홀히 한 행위

18 피심인은 신규 재무관리시스템 서버에 이용자의 주민등록번호 등 개인정보가 포함된 원천징수영수증(PDF파일)을 일시적(10일간)으로 저장하면서, 해당 파일에 포함되어 있는 주민등록번호를 마스킹처리하거나 해당 파일에 비밀번호를 설정 또는 암호화 조치를 하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

19 방송통신위원회는 2019. 10. 1. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요

청하였으며, 피심인은 2019. 10. 15. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

20 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.

21 소득세법 제145조제2항은 "기타소득을 지급하는 원천징수의무자는 이를 지급할 때에 그 기타소득의 금액과 그 밖에 필요한 사항을 적은 기획재정부령으로 정하는 원천징수영수증을 그 소득을 받는 사람에게 발급하여야 한다."라고 규정하고 있고, 소득세법시행령 별지 제23호 서식에서 소득자의 사업자등록번호 또는 주민등록번호를 필요한 사항으로 규정하고 있다.

22 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.

23 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매

출액이 100억원 이상인 정보통신서비스 제공자의 경우 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'를 하여야 한다."고 규정하고 있다.

24 시행령 제15조제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '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.

25 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 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 있고, 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.

26 제6조제2항은 "정보통신서비스 제공자등은 계좌번호 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다."라고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

27 '고시 해설서'는 고시 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 있고, 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 해설하고 있다.

28 고시 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 112비트 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 있고, 제4항에 대해 이용자의 개인정보를 업무용 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호알고리즘이 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.

29 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. 보안메일 열람 시 이용자의 주민등록번호를 사용한 행위{정보통신망법 제23조의2(주민등록번호의 사용제한)중 수집·이용}

30 피심인은 소득세법 제145조제2항에 따라 원천징수의무자로서 기타소득 원천징수영수증 발급을 목적으로 소득자의 주민등록번호 수집·이용이 허용되는 경우에 해당한다. 그러나 피심인이 소득세법 제145조에서 허용한 주민등록번호 수집·이용 목적을 벗어나 보안메일 비밀번호로 주민등록번호 뒤 7자리를 사용한 행위는 정보통신망법 제23조의2제1항을 위반한 것이다.

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

31 **(망분리)** 피심인이 개인정보취급자 그룹의 권한 변경, 개인정보 파일 다운로드가 가능한 개인정보취급자의 컴퓨터 등 내부망을 외부 인터넷망과 서로의 영역에 접근할 수 없도록 물리적이나 논리적으로 망분리하여 차단하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제3호, 고시 제4조제6항을 위반한 것이다.

32 **(열람권한)** 피심인이 해당 기능 또는 시스템을 개발한 후 실제 테스트 수행 및 개인정보에 대한 위험요소를 분석하는 등 보안대책을 마련하지 않아 취급중인 개인정보가 열람권한이 없는 자에게 공개되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

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

33 피심인이 이용자의 주민등록번호 등 개인정보가 포함된 원천징수영수증(PDF파일)을 신규 재무관리시스템 서버에 일시적(10일간)으로 저

장하면서, 해당 파일에 포함되어 있는 주민등록번호를 마스킹처리하거나 해당 파일에 비밀번호를 설정 또는 암호화 조치를 하지 않은 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)
	수집 이용	§23의2①	-	법령에서 허용된 주민번호 수집·이용을 벗어난 행위
	접근 통제	§28①2호	§15②3호	개인정보 다운로드 및 파기 가능한 개인정보취급자의 컴퓨터를 망분리 적용하지 아니한 행위 (고시§4⑥)
	접근 통제	§28①2호	§15②5호	열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
	암호화	§28①4호	§15④2·4호	이용자의 주민등록번호 등 개인정보에 대해 안전한 알고리즘으로 암호화 하지 않고 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장한 행위 (고시§6②)

Ⅳ. 시정조치 명령

1. 시정명령

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

35 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)개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분

리 적용할 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)이용자의 주민등록번호, 여권번호, 계좌번호, 외국인등록번호, 신용카드번호 등 개인정보는 안전한 암호알고리듬으로 암호화하여 저장할 것 4)이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화할 것

2. 시정명령 이행결과의 보고

36 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

37 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.

38 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(방송통신위원회 고시 제2019-12호, 이하 '과징금 부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

39 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

40 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.

41 이에 따를 때, ▲정보통신망법 제28조제1항제2호에 따른 접근통제 중 기술적·관리적 보호조치 중 접근통제 및 개인정보 암호화 조치를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

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

43 과징금 부과기준 제5조제3항 단서조항은, 위반행위의 결과가 ▲위반 정보통

신서비스 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.

44 이에 따라, 피심인의 위반행위의 결과가 ▲개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점, ▲유출된 개인정보가 피심인이 보유하고 있는 개인정보의 100분의 5 이내인 점 등을 종합적으로 고려할 때, '중대한 위반행위'로 판단한다.

3) 기준금액 산출

45 피심인의 서비스 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 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

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

47 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

48 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.

49 이에 따를 때, 피심인이 ▲개인정보 유출사실을 자진 신고한 점, ▲조사에 성실히 협조한 점 ▲개인정보보호관리체계(PIMS) 인증을 획득·유지하고 있는 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 원을 감경한다.

2. 과징금의 결정

50 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 이하에 해당하여 십만원 미만을 절사한 27,200,000원을 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 (20%, 천원)	**2,720만원**
	→ 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

51 피심인의 정보통신망법 제23조의2(주민등록번호의 사용 제한)제1항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제2호·제3호, 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

52 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
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.

53 이에 따라 피심인의 정보통신망법 제23조의2제1항 위반행위에 대해서는 가중하지 않고, 정보통신망법 제28조제1항 위반행위에 대해서는 위반행위별 각 목의 세부기준에서 정한 행위가 2개이므로 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 내부관리계획의 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 컴퓨터바이러스에 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.

54 이에 피심인은 ▲시정조치(안) 사전 통지 및 의견제출 기간 내에 법규 위반 행위에 대하여 시정을 완료한 점 ▲개인정보보호관리체계(PIMS) 인증을 획득·유지하고 있는 점 등을 고려하여 기준금액의 50%인 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§23의2①	1,000만원	없음	500만원	**500만원**
§28①2·4호	1,000만원	300만원	500만원	**800만원**
계				**1,300만원**

다. 최종 과태료

55 이에 따라 피심인의 정보통신망법 제23조의2제1항, 제28조제1항 위반행위에 대해 13,000,000원의 과태료를 부과한다.

Ⅶ. 결론

56 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제2호·제3호(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」 제

20조의 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)