

방 송 통 신 위 원 회

심의 · 의결

안전번호 제2020 - 33 - 160호

안 건 명 개인정보 및 위치정보 보호 법규 위반사업자에 대한 시정조치에
관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020. 6. 4.

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. 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 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기



적으로 확인·감독할 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

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 판매 중개 사이트()를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 매출액 : 피심인이 제출한 자료

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. 2. 26. ~ 2019. 2. 27.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

3. 피심인은 온라인 판매중개 사이트()를 운영하면서 2019. 2. 26. 현재 이용자 명의 개인정보를 수집하여 보관하고 있다.

〈 피심인의 개인정보 수집 현황 〉

구분	항목	수집일	건수
이용자정보			건
합 계			건

나. 개인정보 유출경위

1) 개인정보 유출 경과 및 대응

- 2018.10.12. 17:44 피심인은 신원 미상의 해커로부터 대표 이메일을 통해 고객정보를 해킹하여 보관하고 있으며 삭제 대가로 암호화폐를 요구하는 협박성 1차 이메일을 수신함
- 2018.10.13. 13:26 피심인은 신원 미상의 해커가 보낸 2차 협박 메일을 수신함
- 2018.10.15. 09:10 피심인 담당자는 신원 미상의 해커가 보낸 이메일을 확인하여 유출 가능성을 인지함
- 2018.10.15. 16:24 피심인은 개인정보보호 포털(i-privacy.kr)에 개인정보 유출 사실을 신고함
- 2018.10.15. 18:55 피심인은 개인정보 유출이 의심되는 이용자 명에게 유출 가능성 안내 문자메시지를 발송하고, 웹사이트에 유출 가능성을 공지함
- 2018.11.06. 피심인은 기존에 운영하던 임대서버는 해지하고 과 웹사이트를 재구축하는 계약 체결
- 2019.01.18. 피심인은 신규 웹사이트 오픈

2) 개인정보 유출 규모

4. 피심인이 판매 중개 사이트()를 운영하면서 수집한 이용자의 회원정보 최소 3만여건을 미상의 해커(이하 '이 사건 해커'라



한다.)가 외부로 유출한 것으로 추정된다. 유출된 개인정보 항목은 ,
아이디, 비밀번호, 이름, 닉네임, 생년월일, 이메일, 주소, 우편번호, 일반전화번호,
등으로 추정된다.

3) 개인정보 유출 경로

5. 피심인은 2018. 10. 15. 09:10, 이 사건 해커가 암호화패를 요구하는 이메일을 확인하고 2018. 10. 15. 16:24, 개인정보 유출을 신고하였고, 2018. 10. 15. 18:55 이용자 명에게 유출 가능성에 대한 문자메시지 발송 및 홈페이지에 공지하였으며, 유출당시('18.10.15) 운영하던 임대서버를 해지하여 로그기록이 남아 있지 않아 개인정보 유출 여부 및 경로를 확인할 수 없었다.

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보처리시스템의 접근통제를 소홀히 한 행위

- 1) 개인정보처리시스템에 열람, 수정, 다운로드 등 접근권한을 구체적으로 차등화 하여 부여하지 않은 행위

6. 피심인은 2019. 1. 18. 홈페이지를 개편하면서 2019. 2. 27. 현재 개인정보처리시스템(관리자페이지) 접근권한을 5명에게 부여하고 있으나, 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화하여 부여하지 않고 계정(ID명:admin) 하나로 운영한 사실이 있다.

- 2) 개인정보처리시스템에 접근권한 부여·변경·말소 내역을 기록하고, 그 기록을 최소 5년간 보관하지 않은 행위

7. 피심인은 개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소에 관한 내역을 기록하여 최소 5년간 보관하지 않은 사실이 있다.



나. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

8. 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록(접속일시·처리내역 등)을 신규 웹사이트 시작일인 2019. 1. 18.부터 보존·관리하고 있으나, 그 기록을 월1회 이상 확인·감독하지 않은 사실이 있다.

다. 처분의 사전통지 및 의견 수렴

9. 방송통신위원회는 2019. 4. 18. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

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)’을 하여야 한다.”라고 규정하고 있다.

10. 정보통신망법 시행령 제15조제2항은 “법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(개인정보 처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’을 하여야 한다.”라고 규정하고 있다.



11. 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 제4조제1항은 “정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.”라고 규정하고, 제3항은 “정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.”라고 규정하고 있다.

12. ‘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 있으며, 제3항에 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

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 ‘접속기록의 위조·변조 방지를 위한 조치(제3호)’를 하여야 한다.”라고 규정하고 있다.

13. 정보통신망법 시행령 제15조제3항은 “법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가



개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)'을 하여야 한다.”고 규정하고 있으며, 제6항은 “개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.”라고 규정하고 있다.

14. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시'라 한다) 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.
15. '고시 해설서'는 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,
16. 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.



다. 정보통신망법 제64조제3항은 “방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자 등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템의 접근통제를 소홀히 한 행위(정보통신망법 제28조 제1항제2호)

1) 개인정보처리시스템에 열람, 수정, 다운로드 등 접근권한을 구체적으로 차등화 하여 부여하지 않은 행위

17. 피심인이 개인정보처리시스템(관리자페이지)에 대한 접근권한을 5명에게 부여하면서 서비스 제공을 위해 필요한 범위에서 구체적으로 그 권한을 차등화 하여 부여하지 않고 하나의 계정을 공용으로 사용한 행위는 정보통신망법 제 28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제1항을 위반한 것이다.

2) 개인정보처리시스템에 접근권한 부여·변경·말소 내역을 기록하고, 그 기록을 최소 5년간 보관하지 않은 행위

18. 피심인이 개인정보처리시스템에 대한 접근권한 부여·변경·말소 내역을 기록 하고, 그 기록을 최소 5년간 보관하지 않은 행위는 정보통신망법 제28조제1항 제2호, 같은 법 시행령 제15조제2항, 고시 제4조제3항을 위반한 것이다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위 (정보통신망법 제28조제1항제3호)



19. 피심인이 개인정보취급자의 개인정보처리시스템(관리자페이지)에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 권한	§28①2호	§15②1호	개인정보처리시스템에 열람, 수정, 다운로드 등 접근 권한을 구체적으로 차등화 하여 부여하지 않은 행위(고시 §4①)
	접근 권한	§28①2호	§15②1호	개인정보처리시스템에 접근권한 부여·변경·말소 내역을 기록하고, 그 기록을 최소 5년간 보관하지 않은 행위(고시 §4③)
	접속 기록	§28①3호	§15③1호	개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위(고시 §5①)

IV. 시정조치 명령

1. 시정명령

20. 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 차등화 하여 부여할 것 2)개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관할 것 3)개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독할 것

2. 시정명령 이행결과의 보고



21. 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

22. 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

23. 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 정보 제공 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.

24. 이에 따라 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 2분의 1까지 감경할 수 있다고 규정하고 있다.

25. 이에 따라 조사 과정 중 법규 위반 행위를 중지하고 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려



하여 기준금액의 50%인 500만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2·3호	1,000만원	300만원	500만원	800만원
계				800만원

다. 최종 과태료

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

VII. 결론

27. 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

28. 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.
29. 피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.



30. 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 4일

위원장 한 상 혁



부위원장 표 철 수



위 원 허 욱



위 원 김 창 룡



위 원 안 형 환

