방 송 통 신 위 원 회
심의 · 의결

안건번호 제2020-23-110호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020년 4월 29일

주 문

1. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

2. 피심인은 이용자의 동의를 받은 개인정보의 수집 및 이용·목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

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 과태료를 부과한다.

가. 금　　액 : 5,000,000원

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 홈페이지 제작 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.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수('19.7.30. 기준)

< 피심인의 최근 3년간 매출액 현황 >

(단위 : 천원)

구　분	2016년	2017년	2018년	평 균
매출액				

※ 매출액 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

2 방송통신위원회는 개인정보보호 포털(i-privacy.kr, KISA)에 유출신고한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2019. 7. 30. ~ 7. 31.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집 · 이용 현황

3 피심인은 홈페이지 제작 견적문의 게시판을 운영하면서 2019.7.30. 기준 건의 이용자 정보를 수집 · 보관하고 있다.

< 개인정보 수집 · 이용 현황 >

구분	항목	수집일	건수
견적문의	이름, 이동전화번호, 이메일, 회사명		건
견적문의	상동		건
총 계			건

나. 유출 규모 및 항목

4 미상의 해커(이하 참고6에서 '이 사건의 해커'라 한다)로부터 협박메일을 받은 후 ClamAV*를 이용하여 웹쉘 및 바이러스를 삭제하였고, 악성프로그램이 남아있을 경우를 대비하여 운영체계를 재설치하여 사고당시 접속기록이 없어

개인정보 유출여부를 확인할 수 없었다.

* ClamAV : 시스코에서 제공하는 오픈소스 악성코드 검출엔진

다. 유출 신고 및 대응

일시		피심인의 유출 인지·대응
2019.3.15.	11:31	이 사건의 해커로부터 협박 메일 수신하여 **개인정보 유출 인지** (개인정보 DB를 확보했다고 주장하며 금품(3비트코인)을 요구)
	18:00	한국인터넷진흥원에 해킹사고 신고 및 사이버경찰청 신고
	19:02	개인정보보호포털(i-privacy.kr) **개인정보 유출 신고**
		Clamav이용하여 웹쉘 및 바이러스 삭제 후 OS 재설치

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}

5 피심인은 홈페이지 온라인 견적문의 등을 통해 개인정보를 수집하나, DB접속기록과 관리자페이지 접속기록 등 개인정보처리시스템에 대한 접속기록을 저장·관리하지 않았고, 월1회 이상 그 기록을 확인·감독하지 않은 사실이 있다.

나. 수집·이용 목적이 달성된 개인정보를 파기하지 아니한 행위{정보통신망법 제29조(개인정보의 파기)중 목적을 달성한 경우}

6 피심인은 2011. 12. 2.~ 2019. 7. 30.까지 온라인 견적문의 목적으로 개인정보를 수집하였으나 그 목적을 달성(견적 답변 완료) 후에도 개인정보(이름, 이동전화번호, 이메일 주소 등) 5,031건을 파기하지 않고 보관한 사실이 있다.

< 피심인이 파기하지 않고 보관중인 개인정보 항목 >

다. 처분의 사전통지 및 의견 수렴

7 방송통신위원회는 2019. 8. 19. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 8. 28. 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 '접속기록의 위조·변조 방지를 위한 조치(제3호)'를 하여야 한다."라고 규정하고 있다.

8 정보통신망법 시행령 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.

9 시행령 제15조제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."라고 규정하고 있다.

10 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 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상* 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

* 2020.1.2. 시행된 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호)에서는 접속기록을 최소 1년 이상 보존·관리하도록 개정됨

11 '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,

12 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.

* 2020.1.2. 시행된 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호)에는 최소 1년 이상으로 개정

나. 정보통신망법 제29조제1항은 "정보통신서비스 제공자등은 '제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다."라고 규정하고 있으며, 제23조제1항 단서는 "다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다."라고 규정하고 있다.

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

13 피심인이 홈페이지를 통해 개인정보를 수집 시 개인정보처리시스템에 대한 접속기록(식별자, 접속일시, 접속지, 수행업무 등)을 6개월 이상 저장·관리하지 않고, 월1회 이상 그 기록을 확인·감독하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항을 위반한 것이다.

나. 수집·이용 목적이 달성된 개인정보를 파기하지 아니한 행위{정보통신망법 제29조(개인정보의 파기)중 목적을 달성한 경우}

14 피심인이 온라인 견적문의 답변을 목적으로 2011. 12. 2.~ 2019. 7. 30.까지

수집한 개인정보에 대해 답변을 완료하여 그 목적을 달성하였음에도 불구하고 5,031건을 파기하지 않고 보관한 행위는 정보통신망법 제29조제1항제1호를 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시 §5①)
	미파기	§29①1호	-	수집·이용 목적을 달성한 개인정보를 파기하지 않고 보관한 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

나. 피심인은 이용자의 동의를 받은 개인정보의 수집 및 이용·목적을 달성한 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다.

2. 시정명령 이행결과의 보고

15 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하

여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

V. 과태료 부과

16 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

17 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.

18 그러나 피심인은 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

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.

19 이에 따라 조사 과정 중 법규 위반 행위를 중지하고 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 500만원을 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①3호	1,000만원	없음	500만원	**500만원**
계				**500만원**

다. 최종 과태료

20 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 5,000,000원의 과태료를 부과한다.

Ⅵ. 조사결과 수사기관 이첩

21 정보통신망법 제29조(개인정보의 파기)제1항제1호에 따라 정보통신서비스 제공자등은 이용자에게 동의받은 개인정보의 수집·이용 목적 등을 달성한 경우 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 이를 위반하는 경우 같은 법 제73조제1의2호에 따라 2년 이하의 징역 또는 2천만원 이하의 벌금에 해당한다.

22 피심인은 조사당시까지 수집·이용 목적 등을 달성한 이용자의 개인정보 5,031건을 파기하지 않고 보유하고 있어 정보통신망법 제29조(개인정보의 파기)제1항제1호를 위반하는 행위가 있다고 인정된다. 이에 같은 법 제73조제1의2호에 해당되어 조사결과를 수사기관에 이첩한다.

Ⅶ. 결론

23 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호(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」 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.

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)