방 송 통 신 위 원 회
심의 · 의결

안건번호 제2019 - 05 - 022호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2019. 1. 29.

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. 개인정보취급자의 접근권한 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

2. 피심인은 이용자의 개인정보 수집·이용·제공 등의 동의 철회 또는 개인정보의 열람·제공·정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

3. 피심인은 제1항 및 제2항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시

하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

4. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 10,000,000원

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(　　)와 모바일 앱(　　)을 통해　　서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황과 매출액 현황은 다음과 같다.

< 피심인의 일반현황 >

('17.12월말 기준)

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 매출액 현황 〉

(단위 : 억원)

구　분	2015년	2016년	2017년	평 균
매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 기획조사하였고, 피심인에 대한 현장조사(2018.7.20.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ' ' 서비스를 운영하면서 2018. 7. 20. 기준 건의 개인정보를 수집·보관하고 있다.

< 피심인의 개인정보 수집 현황 >

구 분	항 목	수집기간	건수
개인정보 (회원)			

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

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

(접근권한 기록보관) 피심인은 개인정보처리시스템에 대하여 개인정보관리책임자 및 개인정보취급자의 접근 권한 부여 및 변경 또는 말소에 관한 내역을 기록·보관하지 않은 사실이 있다.

(안전한 인증수단) 피심인은 개인정보취급자가 외부인터넷망을 통해 관리자

페이지(　　)에 접속 시 아이디와 패스워드 외에 OTP 등 추가적인 안전한 인증수단 없이 접속이 가능하도록 한 사실이 있다.

나. 이용자의 개인정보 수집·이용·제공 등의 동의 철회{정보통신망법 제30조(이용자의 권리 등) 중 개인정보 동의 철회}**를 어렵게 한 행위**

피심인은 홈페이지　　및 앱　　을 통해 이용자가 쉽게 회원 가입할 수 있도록 하고 있으나 회원탈퇴를 위한 별도 페이지는 마련되어 있지 않고 전화 상담을 통해서만 회원탈퇴가 가능하도록 한 사실이 있다.

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)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)' 등의 조치를 하여야 한다."라고 규정하고 있으며, 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) 고시 제4조제3항은 "정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다."라고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."고 규정하고 있다.

'고시 해설서'는 고시 제4조제3항에 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 있고, 제4항에 대해 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 필요하다"고 해설하고 있다.

나. 정보통신망법 제30조제1항은 "이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다."라고 규정하고 있고, 제6항은 "정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법 보다 쉽게 하여야 한다."라고 규정하고 있다

'정보통신망법 해설서'는 ▲"이용자가 회원탈퇴나 서비스 이용 계약 해지 등 동의철회를 하는 방법은 회원가입 등 개인정보를 수집하는 방법보다 어려워서는 안 되며 더 쉬운 방법인지 여부는 구체적인 사안별로 접근매체의 다양성을 고려하여 개별적으로 판단하여야 하지만, 일반적으로 철회방법이 수집 시와 동일한 방법으로 제공되고 이에 더하여 추가적인 조치가 제공되는 경우 더 쉬운 방법으로

인정될 수 있으며 추가적인 조치로는 접근매체 확대(전화, ARS, 이메일 등을 통한 철회도 가능하도록 조치), 철회 메뉴의 다양화(철회메뉴를 메인화면 외에 개인정보처리방침, 나의 개인정보, 해당 서비스의 게시판 등에서 언제든지 쉽게 발견하고 신청할 수 있도록 조치) 등을 고려할 수 있으며 이는 일부 사업자들이 회원가입 절차는 쉽게 하면서도 탈퇴 절차는 까다롭게 만들어 이용자의 개인정보를 악용하는 경우를 방지하기 위함입니다."라고 해설하고 있다.

또한 ▲ "동의철회뿐만 아니라 개인정보를 열람하고 정정하는 절차도 개인정보 수집절차보다 쉬워야 합니다."라고, ▲ "동의철회나 열람·정정 방법은 이용자가 언제든지 쉽게 확인 할 수 있도록 개인정보취급방침을 통해 안내하여야 합니다."라고 설명하고 있다.

다. 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**

(접근권한 기록보관) 피심인이 개인정보처리시스템에 대하여 개인정보취급자에 대한 권한부여 및 변경 또는 말소에 대한 내역을 기록하고 최소 5년 이상 보관하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

(안전한 인증수단) 피심인은 개인정보취급자가 외부에서 피심인의 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고

추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않았다. 이러한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

나. 이용자의 개인정보 수집·이용·제공 등의 동의 철회{정보통신망법 제30조(이용자의 권리 등) 중 개인정보 동의 철회}**를 어렵게 한 행위**

피심인이 홈페이지 및 앱 를 통해 이용자가 쉽게 회원 가입할 수 있도록 하고 있으나 회원탈퇴를 위한 별도 페이지는 마련되어 있지 않고 전화 상담을 통해서만 회원탈퇴가 가능하도록 한 행위는 정보통신망법 제30조제6항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	개인정보취급자에 대한 권한 부여·변경·말소내역을 기록하고 그 기록을 최소 5년간 보관하지 아니한 행위(고시§4③)
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	이용자 권리	§30⑥		개인정보의 수집방법 보다 동의철회 방법을 어렵게 한 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 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) 개인정보취급자의 접근권한 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

나. 피심인은 이용자의 개인정보 수집·이용·제공 등의 동의 철회 또는 개인정보의 열람·제공·정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 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 제28조(개인정보의 보호조치)제1항, 제30조제6항(이용자의 권리 등) 위반행위에 대한 과태료는 같은 법 제76조제1항제3호·제5호, 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

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
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
러. 법 제30조제3항·제4항 및 제6항(법 제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 않은 경우	법 제76조 제1항제5호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸·조작, 허위 정보 제공 등 조사방해, ▲위반의 정도, ▲ 기타 위반행위의 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, 과태료 부과지침 제8조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

그러나 피심인의 정보통신망법 제28조제1항, 제30조제6항 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 가중하지 않는다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자의 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲ 조사협조와 자진시정 ▲기타 위반행위의 정도, 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우에는 과태료 부과지침 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항, 제30조제6항 위반행위에 대해서 시정조치(안) 사전 통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료한 점을 고려하여 기준금액의 50%인 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	1,000만원	없음	500만원	**500만원**
§30⑥	1,000만원	없음	500만원	**500만원**
계				**1,000만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항, 제30조제6항 위반행위에 대해 1,000만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호·제5호(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.

2019년 1월 29일

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)