개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2022-008-052호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

의결연월일 2022. 5. 11.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리 시스템에 대한 접속 권한을 아이피(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

2) 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 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 을 운영하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 가 자사 개인정보 판매 게시글이 다크웹에서 확인되어 유출신고(2021.9.29.)함에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021.10.6. ~ 2021.12.15.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 제공하면서 '21. 12. 3. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'21. 9. 28.	12:30	보안담당자가 한국인터넷진흥원에서 보낸 개인정보 다크웹 게재 관련 메일을 확인
	14:00	데이터베이스 외부 접속 차단 및 데이터베이스 암호 변경
	16:50	다크웹에 공개된 샘플데이터 고객정보 확인 및 개인정보 유출 인지
	16:55~	개인정보 유출 관련 시스템 취약점 조치 및 원인 분석
'21. 9. 29.	13:00	한국인터넷진흥원에 개인정보 유출 신고
	17:00	이용자 전체를 대상으로 유출 사실 통지(이메일)
	17:40	홈페이지를 통해 개인정보 유출 사실 공지

2) 유출규모 및 경위

(유출항목 및 규모) ’21. 9. 28.에 신원 미상의 자(이하 ‘해커’)가 다크웹에 공개한 개인정보 건*

* 아이디, 암호화 비밀번호, 이름, 이메일, 핸드폰번호, 생년월일 등

(유출경위) 피심인이 접근 아이피(IP)를 제한하지 않아 해커가 알 수 없는 방법으로 획득한 데이터베이스 계정으로 데이터베이스 서버에 무단 접근하여 개인정보를 유출한 것으로 추정

※ 조사 결과, 현장 조사(‘21.10.5.) 시 가 보유한 회원정보는 만건으로 해커가 보유한 것으로 주장하는 개인정보 수치(만 건)와 유사하였음. 또한, ’21.9.22.에 대량의 정보 전송(약 102Mb/초)이 발생하였고 ‘21.4.26에 미국 아이피(IP)에서 비정상 접속 시도가 있었으나, 세부 로그가 없어 전송된 정보 내 개인정보 포함 여부, 로그인 성공 여부 등은 확인이 불가함

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입차단·탐지시스템을 설치·운영하였으나 ‘21. 7. 27.부터 ’21. 9. 28.까지 접근 아이피(IP)를 제한하지 않고 운영하여 이용자의 개인정보가 유출된 사실이 있다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

피심인은 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록*을 보존·관리하지 않은 사실이 있다.

* 피심인은 데이터베이스에 대한 에러로그만 보관하고 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지, 수행 업무 등을 확인할 수 있는 일반 로그는 기록하지 않도록 설정·운영함

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 12. 28. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2022. 1. 12. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

제48조의2제1항제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하

‘고시’라 한다) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있다.

고시 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존.관리하여야 한다.” 라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위[보호법 제29조(안전조치의무) 중 불법적인 접근 차단]

1) (침입차단 및 탐지시스템의 운영) 피심인이 개인정보처리시스템에 대한 접근권한을 개인정보취급자에게 허용된 아이피(IP)로 제한하지 않고, 외부 인터넷 어디서나 접속할 수 있도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2 제1항제2호, 고시 제4조제5항을 위반한 것이다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위[보호법 제29조(안전조치의무) 중 접속기록의 위조 · 변조 방지를 위한 조치]

피심인이 개인정보가 저장되는 데이터베이스 서버에 접속하는 개인정보취급자의 접속기록을 보존·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2 제1항제3호, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 접속기록)	보호법 §29	§48의2① 제2·3호	• 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위(고시§4) • 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위(고시§5)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 아이피(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

2) 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 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 미부과

피심인의 보호법 제29조 위반행위는 '개인정보보호 법규 위반에 대한 과징금 부과기준'(개인정보보호위원회 고시, 제2020-6호) 제9조의 위반행위가 경미하여 시정

조치로 갈음할 수 있는 경우*에 해당하여 과징금을 미부과하나, 추후 100건 이상의 개인정보 유출이 확인되면 과징금을 부과한다.

* 개인정보 유출규모가 100건 미만으로 피해가 발생하지 않거나 미미한 경우

3. 과태료 부과

피심인의 보호법 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호 및 같은 법 시행령 제63조의〔별표2〕'과태료 부과기준' 및「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 600만원을 적용한다.

<「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과

등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 경우로 기준금액의 %를 가중한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 점 등을 감안하여 과태료 부과지침 제7조에 따라 기준금액의 %를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 접속기록)	600만원			

Ⅴ. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항제6호, 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

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

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 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.

이상과 같은 이유로 주문과 같이 의결한다.

2022년 5월 11일

위 원 장 윤 종 인

부위원장 최 영 진

위 원 강 정 화

위 원 고 성 학

위 원 백 대 용

위 원 염 흥 열

위 원 이 희 정

위 원 지 성 우