개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2022-018-152호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2022. 11. 16.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 3,600,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 서비스를 운영하는「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다)에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보종합포털(privacy.go.kr)에 유출 신고('21. 5. 13.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('21. 7. 7. ~ '22. 3. 21.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 운영하면서 '21. 7. 13. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
‘20. 11. 20.	-	이용자 A 간편 회원가입 완료 - 식별 값이 비정상적(undefined)으로 전송되었으나, 정상 가입 처리됨
‘21. 5. 11.	-	이용자 B 간편 회원가입 시도 - 식별 값이 비정상적(undefined)으로 전송되고, 이용자 A의 계정으로 로그인 처리됨
‘21. 5. 12.	13:42	피심인의 고객센터에 민원 접수
	16:55	담당자 오류내용 확인
	21:00	시스템 개선 완료
‘21. 5. 13.	13:37	개인정보보호 포털에 개인정보 유출 신고
	13:44	전화, 문자메시지를 통하여 이용자에 개인정보 유출 통지

2) 유출규모 및 경위

(유출항목 및 규모) 이용자 1명의 아이디, 휴대전화번호, 주소, 이메일주소

(유출 경위) 이용자가 간편 회원가입 시 알 수 없는 오류로 비정상 식별 값(undefined)이 전송되어 다른 이용자의 계정으로 로그인 처리됨

’20. 11. 20. : 이용자A는 간편 회원가입을 진행하였고, 계정 연동 과정에서 알 수 없는 오류로 인해 으로부터 비정상 식별 값(undefined)을 전송받아, 시스템에 이용자A의 식별 값이 비정상 값인 ‘undefined’로 그대로 저장되고 회원가입이 완료됨

’21. 5. 11. : 이용자B가 간편 회원가입을 진행하였으나, 계정연동 오류로 으로부터 비정상 식별 값(undefined)을 전송받으면서 회원가입 되지 않고, 동일한 식별 값(undefined)으로 저장되어 있던 이용자A의 계정으로 로그인 처리되어 이용자A의 개인정보가 이용자B에게 조회됨

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 이용자 편의를 위하여 SNS 간편 회원가입 및 로그인 기능을 제공하면서, 간편 회원가입 시 이용자 식별 값에 대한 유효성 검증을 하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’22. 3. 28., ‘22. 10. 31. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ‘22. 4. 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 접근통제를 위하여 필요한 조치(마목)를 하여야 한다.”라고 규정하고 있다.

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

같은 법 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보 취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 하지 않은 행위[보호법 제29조(안전조치의무) 중 접근통제]

피심인이 비정상적인 식별 값에 대한 유효성 검증을 하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48조의2① 제2호	• 처리중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치를 소홀히 한 행위(고시§4⑨)

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호, 같은 법 시행령 제63조의 [별표2] '과태료 부과기준' 및「개인정보 보호법 위반에 대한 과태료 부과기준(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과기준'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, 제28조의4 제1항 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 부과기준 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 있다'라고 규정하고 있다.

피심인의 경우 법 위반상태의 기간이 3개월 이상인 경우에 해당하여 기준금액의 10%를 가중한다.

2) **(과태료의 감경)** 과태료 부과기준 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 있다'라고 규정하고 있다.

피심인의 경우 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위에 대한 시정을 완료한 점, 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점을 고려하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 360만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	60만원	300만원	**360만원**

3. 결과 공표

보호법 제66조제1항 및 「개인정보보호위원회 처분결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 위반행위 시점을 기준으로 위반 상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표 개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
명칭	위반조항	위반내용	처분일자	처분내용
	법 제29조	안전조치의무	2022. 11. 16.	과태료 부과 360만원

Ⅴ. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항 제6호, 제66조(결과의 공표)제1항에 따라 과태료, 결과 공표를 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.

2022년 11월 16일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)