

개 인 정 보 보 호 위 원 회

심의 · 의결

의 안 번 호 제2023-004-020호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의 결 연 월 일 2023. 3. 8.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 「개인정보보호법」(이하 “보호법”이라 한다.) 제2조제6호에 따른 공공기관으로, 00자원 발굴, 보존, 수집, 연구 등을 주 업무로 하는 보호법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 관리수준 진단 미흡기관에 대한 개인정보 관리실태 조사('22. 11. 28. ~ 30)를 통해 피심인의 개인정보 보호법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용

피심인은 생물자원의 분양 신청 접수 및 관리를 위해 000자원통합정보 시스템을 운영하면서 '22. 11. 28. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

< 개인정보 수집현황 >

구분	수집·이용 항목	수집일	건수(명)
개인정보파일정보	(필수) 이름, 이메일, 휴대전화번호, 직장연락처, 직장주소, 영문명ID, 기관명, 부서명	'22. 1 7. ~	110명* (110건)

* 정보주체(4명), 외부 과제참여자, 내부직원을 합한 수치

나. 개인정보의 취급·운영 관련 사실관계

1) 개인정보에 대한 안전조치의무를 소홀히 한 행위

피심인은 000자원통합정보시스템 관리자계정의 비밀번호 변경시 비밀번호 작성규칙을 수립·적용하지 않은 사실이 있다.

피심인은 개인정보취급자가 정보통신망을 통해 외부에서 000자원통합정보시스템에 접속하려는 경우 안전한 접속수단이나 안전한 인증수단을 적용하지 않은 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 1. 27. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 9. 위반 사실을 인정하고 위반사항에 대해 전부 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

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

같은 법 시행령 제30조제1항은 안전성 확보조치로 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(2호)를 하도록 하고 있다.

같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’라고 한다.)에서는 “개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.(제5조제5항)”, “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.(제6조제2항)”고 규정하고 있다.

나. 위법성 판단

피심인은 개인정보처리자로서 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 하나, 000자원통합정보시스템 관리자계정의 비밀번호 변경시 비밀번호 작성규칙을 수립·적용하지 않아 1자리 이상 단순 비밀번호로도 변경 가능하게 한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제2호, 고시 제5조제5항을 위반한 것이다.

피심인은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단이나 안전한 인증수단을 적용하여야 하나, 외부에서 000자원통합정보시스템에 접속하려는 경우 안전한 인증수단을 적용하지 않아 아이디와 비밀번호만으로 로그인 가능하도록 한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제2호, 고시 제6조2항을 위반한 것이다.

IV. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반에 대한 과태료는 같은 법 제75조(과태료)제2항제6호 및 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」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 제29조(안전조치의무) 위반에 대해서 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 과태료 부과기준, 개인정보보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보보호법 위반에 대한 과태료 부과기준」(개인정보위 2021. 1. 27. 이하 '과태료 부과지침') 제8조(과태료의 가중)는 '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 보호법 제29조(안전조치의무) 위반행위는 과태료 부과지침 제8조의 과태료 가중기준에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 2개인 점을 고려하여 기준금액의 10%인 60만원을 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개에 해당하는 경우	기준금액의 50% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

다. 과태료의 감경

과태료 부과지침 제7조(과태료의 감경)는 ‘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, 사전통지 및 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정을 완료한 점, 조사 기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 적극 협력한 점 등을 종합적으로 고려하여 과태료 부과지침 제7조의 과태료 감경기준에 따라 기준금액의 50%를 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조· 자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

라. 최종 과태료

피심인의 개인정보 보호법 제29조를 위반한 행위에 대하여 기준금액에서 가중·감경을 거쳐 총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B+C)
제29조(안전성확보 조치 의무 위반)	법 제75조제2항제6호	600	60	△300	360

V. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제75조 (과태료)제2항제6호에 의한 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

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

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.