개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2024-003-036호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2024. 2. 14.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」(이하 ‘보호법’이라 한다) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 관리수준 진단 미흡기관에 대한 개인정보 관리실태 현장조사( )를 통해 피심인의 개인정보 보호법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집.이용 현황

피심인은 을 위해 ‘ ’를 운영하면서 기준 아래와 같이 개인정보를 수집 · 보유하고 있다.

개인정보파일	수집·이용 항목	수집일	보유건수(명)

나. 개인정보 취급·운영 관련 사실관계

1) 개인정보에 대한 안전조치의무를 소홀히 한 행위

피심인은 ’ 시스템‘의 관리자페이지에 개인정보취급자가 외부에서 접속하려는 경우 안전한 인증수단을 적용하여야 하나 아이디와 비밀번호만으로 접속이 가능하도록 운영한 사실이 있으며, 회원이 로그인을 위해 외부에서 비밀번호를 입력·송신하는 경우에 이를 암호화하지 않은 사실이 있고, 접속기록 중 아이디, 수행업무, 처리한 정보주체 항목을 보관·관리하지 않은 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며 피심인은 위반 사실을 인정하며 선처를 요청하였다.

Ⅲ. 위법성 판단

1. 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 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.”라고 규정하면서 “개인정보처리자는 개인정보에 대한 접근을 통제하기 위한 조치(3호)”, “개인정보를 안전하게 저장·전송하는데 필요한 조치(4호)”, “개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(5호)”를 하도록 규정하고 있다.

같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2023-6호, 이하 ‘고시’) 제6조제2항은 “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다.”라고 규정하고 있으며, 고시 제7조제1항은 “개인정보처리자는 비밀번호, 생채인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다.”라고 규정하고 있고, 고시 제8조제1항은 “개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다.”라고 규정하고 있으며, 고시 제2조제3호는 “접속기록’이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

1) 접근통제를 소홀히 한 행위

개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서 등 안전한 인증수단을 적용하여야 하나, 피심인이 개인정보취급자가 정보통신망을 통해 외부에서 ‘ 시스템’에 아이디 · 비밀번호만으로 접속이 가능하도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제6조제2항을 위반한 것이다.

2) 개인정보의 암호화를 소홀히 한 행위

개인정보처리자는 비밀번호 등 인증정보를 정보통신망을 통해 송 · 수신하는 경우 이를 안전한 알고리즘으로 암호화하여야 하나, 피심인이 ‘ 시스템’ 회원의 로그인 비밀번호 송신 시 이를 암호화하지 않은 행위는 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제7조제1항을 위반한 것이다.

3) 접속기록의 보관 및 점검을 소홀히 한 행위

개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록(식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등)을 1년 이상 보관 · 관리하여야 하나, 피심인이 ‘ 시스템’에서 개인정보취급자의 아이디, 수행업무, 처리한 정보주체 항목을 보관·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제30조제1항, 고시 제8조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	세부내용
안전조치의무 위반	보호법 §29	·개인정보취급자가 외부에서 정보처리시스템 접속하려는 경우 안전한 인증수단을 적용하지 않은 행위 ·정보통신망을 통하여 정보주체의 비밀번호를 송신하는 경우에 이를 암호화하지 않은 행위 ·개인정보취급자의 아이디, 수행업무, 처리한 정보주체 항목을 보관·관리하고 있지 않은 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대해 같은 법 제75조제2항제5호, 같은 법 시행령 제63조의 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회지침 2023.9.15., 이하 '과태료 부과지침')에 따라 다음과 같이 과태료를 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 아래의 위반행위에 대해 1회 위반에 해당하는 금액 600만 원을 적용한다.

< 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
아. 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제5호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

과태료 부과지침 제7조는 "위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반 주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다"라고 규정하고 있다.

피심인의 보호법 제29조 위반행위는 과태료 부과지침 제7조 [별표3]의 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우'로서 기준금액의 30%인 180만 원을 가중한다.

< 과태료 가중기준 >

기준	가중사유	가중비율
위반 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우	기준금액의 30% 이내

2) 과태료의 감경

과태료 부과지침 제6조는 "위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보처리자의 업무 형태 및 규모, ▲개인정보보호 인증, ▲자율규제 규약 등, ▲개인정보보호 활동, ▲조사 협조, ▲자진 시정 등, ▲피해 회복·피해 확산 방지, ▲자진 신고)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다."라고 규정하고 있으며, "감경 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다."라고 규정하고 있다.

피심인이 조사 기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점, 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 점 등을 종합적으로 고려하여, 과태료 부과지침 제6조 [별표2] 감경기준에 따라 기준금액의 40%인 240만 원을 감경한다.

< 과태료 감경기준 >

기준	감경사유	감경비율
조사 협조	보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액 20% 이내
자진 시정	과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액 20% 이내

다. 최종 과태료

피심인의 보호법 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 540만 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 (안전조치의무 위반)	법 제75조 제2항제5호	600	180	240	540

Ⅴ. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조제2항제5호에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

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(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.