개 인 정 보 보 호 위 원 회

제 2 소 위 원 회

심의·의결

안 건 번 호 제2024-223-713호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (고유번호 :)

대표자

의결연월일 2024. 11. 27.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 4,500,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 에 따라 설립된 법인으로, 「개인정보 보호법」(이하 '보호법'이라 한다) 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	고유번호	대표자 성명	주소

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출 신고(2023. 8. 23.)에 따라 조사를 실시하였으며(2023. 8. 24. ~ 2023. 12. 15.), 피심인의 법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 를 위해 2023. 8. 20. 기준으로 아래와 같이 개인정보를 수집·보관하였다.

구분	항 목	기간	건수

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

피심인이 운영하는 홈페이지 회원 12,131명의 개인정보가 유출되었으며, 유출항목별로는 이름·휴대폰번호는 1,714명, 이름·이메일주소는 9,776명, 이름·주소는 641명이다.

2) 유출 경위

2023. 8. 20. 신원 미상의 자(IP:)가 피심인의 홈페이지 DBMS 관리자 페이지( )에 로그인하여 회원정보가 담긴 데이터베이스를 삭제하고, 테이터베이스 복구를 위해서는 비트코인을 입금하라는 내용이 담긴 DB 테이블을 신규로 작성하였다. 관리자 계정(root)의 비밀번호가 설정되어 있지 않아, 위 신원 미상의 자가 비밀번호 입력 없이 로그인에 성공한 것으로 추정된다.

3) 유출인지 및 대응

일시			유출 인지 및 대응 세부내역
2023.	8.20.	18:00	홈페이지 접속 불가 확인하여 유지보수업체에 오류 확인 요청
	8.21.	08:40	유지보수업체로부터 해킹으로 인해 DB가 삭제되었다는 통보를 받고 **개인정보 유출 인지**
	8.22.		정보주체에게 **유출 통지*** 및 홈페이지 내 개인정보 **유출 통지문 게시** * 문자 1,749건(20:00), 이메일 500건(21:06)
	8.23.	21:28	개인정보포털에 개인정보 **유출 신고**
	8.24.		정보주체에게 **추가 유출 통지*** * 우편 915건, 이메일 17,683건
	9.14.		웹 취약점 점검
	10.1.		로컬서버 접근만 가능하도록 조치
	10.10.		IDC센터 내 방화벽 및 웹방화벽 설치
	12.15.		회사 내 방화벽 VPN 설치
2024	2.27.		통합전산센터 입주

※ (유출건수와 통지건수 불일치 사유) 유출 인지 시점의 유출건수는 20,459건으로 추정되었으나, 유출 통지 과정에서 전화번호 해지, 잘못된 집주소 또는 이메일 주소로 우편물 반송 등 사유 확인된 건(8,328건)을 제외한 최종 유출건수는 12,131명으로 확정

3. 개인정보의 취급·운영 관련 사실관계

피심인은 홈페이지 DBMS 관리자 계정의 비밀번호를 설정하지 않아, 비밀번호 입력 없이 데이터베이스에 접근이 가능하도록 방치하였으며, 홈페이지를 통해 개인정보를 처리하면서 방화벽, 웹방화벽 등 침입차단 및 침입탐지 시스템을 설치·운영하지 않았을 뿐만 아니라, 정보통신망을 통한 외부 접속 시 안전한 접속수단 또는 인증수단을 적용하지 않고 아이디와 비밀번호 입력만으로 로그인이 가능하도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2024. 1. 2. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2024. 1. 8. 방화벽 및 웹방화벽을 설치하고 관리자 계정은 로컬서버 접근만 허용하는 등 안전성 강화를 위한 시정조치를 완료하였으므로 선처를 구한다는 의견을 개인정보보호위원회에 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

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 있고, 같은 법 시행령[1] 제30조제1항제2호는 “개인정보에 대한 접근 권한을 제한하기 위해 ‘정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영(나목)’을 해야 한다“라고 규정하고 있다. 또한 시행령 제30조제1항제3호는 ”개인정보에 대한 접근을 통제하기 위해 ‘개인정보처리

1) 대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행

시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)' 및 '그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)'를 해야 한다"라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준[2]」(이하 '안전성 확보조치 기준') 제5조제5항은 "개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다"라고 규정하고 있고, 제6조제1항은 "개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)'하고, '개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응(제2호)'을 하여야 한다"고 규정하고 있으며, "개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다"라고 규정하고 있다.

2. 위법성 판단

피심인이 '21. 1. 1.부터 '23. 10. 1.까지 홈페이지 DBMS 관리자 계정의 비밀번호를 설정하지 않은 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제2호 및 안전성 확보조치 기준 제5조제5항을 위반한 것이고, 같은 기간 정보통신망을 통해 외부에서 홈페이지 DB 관리자 페이지에 접속할 때 안전한 인증수단을 적용하지 않고 아이디와 비밀번호만 입력하여 접속이 가능하도록 한 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제3호 및 안전성 확보조치 기준 제6조제2항을 위반한 것이다.

또한, 피심인이 '21. 1. 1.부터 '23. 10. 10.까지 홈페이지를 통해 개인정보를 처리하면서 방화벽·웹방화벽 등 침입 차단 및 침입 탐지 시스템을 설

2) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

치·운영하지 않은 행위는 법 제29조, 같은 법 시행령 제30조제1항제3호 및 안전성 확보조치 기준 제6조제1항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대해 같은 법 제75조제2항제5호 및 같은 법 시행령 제63조 [별표2] 제2호아목 및 「개인정보 보호법 위반에 대한 과태료 부과기준」(지침, 2023. 9. 15. 시행, 이하 '과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있는바, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 피심인의 위반행위에 대해 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 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 "결과와 당사자의 위반행위의 정도, 위반행위

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

피심인의 경우 ▲시행령 [별표2] 제2호아목의 위반행위가 과태료 부과지침 [별표3] 제3호의 세부기준에서 정한 행위 중 2개에 해당하고(15%), ▲법 위반 상태의 기간이 ’21. 1. 1.부터 ’23. 10. 10.까지로서 2년을 초과(30%)하는 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액에 45%를 가중한다.

< 과태료의 가중기준 >

기준	감경사유	감경비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 15% 이내
위반기간	1. 법 위반 상태의 기간이 2년을 초과하는 경우	기준금액의 30% 이내

2) 과태료의 감경

과태료 부과지침 제6조는 ”당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다(제1항)“라고 규정하면서, ”[별표2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 제2호 1) 및 2)에 해당하는 사유가 각 2개 이상 해당되는 경우에는 기준 금액의 100분의 50을 초과할 수 없고, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다“라고 규정하고 있다.

피심인의 경우 ▲비영리법인으로서 소관 업무의 성격이 공익성 및 비영리성을 띠는 점(30%), ▲조사기간 중 일관되게 행위사실을 인정하면서 조사에 적극 협력한 점(20%), ▲과태료의 사전통지 및 의견제출 기간 내에 위반행위의 시정을 완료한 점(20%)을 고려하여 과태료 부과지침 제6조에 따라 기준금액의 70%를 감경한다.

< 과태료의 감경기준 >

기준	감경사유	감경비율
1) 당사자의 환경 및 위반 정도 등 : 기준금액의 50% 이내		
개인정보처리자의 업무형태 및 규모	1. 위반행위자가 비영리법인, 비영리단체 등인 경우로서 무보수성, 공익성, 비영리성 등을 고려할 때 과중하다고 인정되는 경우	기준금액의 30% 이내
2) 개인정보 보호 노력, 조사 협조·자진 시정 등 : 기준금액의 50% 이내 **(2) 조사 협조, 자진 시정 등**		
조사협조	보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 20% 이내
자진시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 20% 이내

다. 최종 과태료

피심인의 법 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 450만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치 의무 위반	600만 원	270만 원	420만 원	**450만 원**

Ⅴ. 결론

피심인의 보호법 제29조 위반 행위에 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납부 의무를 부담한다.