개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-016-236호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (재)전남테크노파크 (사업자등록번호 :)

의결연월일 2025. 7. 23.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 98,000,000원

   나. 과 태 료 : 3,600,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 처분 등을 받은 사실을 다음과 같이 공표할 것을 명한다.

   가. 피심인은 처분 등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분 등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만의 기간 동안(휴업일 포함) 게시할 것

나. 피심인은 원칙적으로 표준 공표 문안을 따르되, 공표 문안에 관하여 개인정보보호위원회와 미리 문서로 협의해야 하며, 팝업창 설정방식 및 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 개인정보보호위원회와 협의하여 정할 것

이 유

Ⅰ. 기초 사실

피심인은 지역 중소기업 육성을 위하여 전남도청 등이 출연하는 「민법」 제32조에 따른 비영리 재단법인으로 「개인정보 보호법」(법률 제19234호, 이하 "보호법") 제2조 제5호에 따른 개인정보처리자로서 일반현황은 다음과 같다.

피심인명	사업자등록번호	대표자 성명	주소	직원 수
전남테크노파크				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출 신고('23.11.30.)에 따라 보호법 위반 여부를 조사하였으며, 그 결과 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 회원관리를 위하여 '24.2.15. 기준으로 아래와 같이 개인정보를 수집·보유하고 있다.

개인정보파일 (개인정보처리시스템)	수집항목	수집 기간	보유 기간	건수

나. 개인정보 유출 관련 사실관계

1) 유출 경위

사고 당시 피심인은 운영 중인 의 DBMS 계정에 유추하기 쉬운 아이디(등)와 비밀번호(등)를 사용하고 있었고, 신원 미상의 자(, 미국, 이하 '해커'라 한다)가 상기 계정 중 일부를 이용하여 외부에서 DB에 불법 접근하여 개인정보를 유출했다고 주장하고 있고, 저장된 개인정보

는 삭제·훼손되었다. 해커는 DB 내에 “너의 DB를 백업했다. 복구하고 싶으면 0.0151 비트코인(한화 75만원 상당)을 요구하는 메시지(랜섬노트)를 남긴 것으로 확인되었다.

2) 유출규모 및 항목

해커가 DB 내 개인정보를 삭제하여, ’23. 7월 홈페이지 기능개선 작업 후 백업한 DB를 통해 유출규모를 산출한 결과 1,261명의 개인정보가 삭제 및 훼손되었고, 삭제된 항목에는 성명, 성별, 외국인 여부, 유선 전화번호, 핸드폰번호, 이메일, 소속기관, 소속부서, 직위, 아이디, 비밀번호, DI가 포함되었다.

3) 유출 인지 및 대응

일시			유출 인지 및 대응 내용
2023	11. 23.	14:00	▸ 운영담당자가 홈페이지 접속 불가를 확인하고 서버 긴급 점검
		15:00	▸ 해커가 DB의 개인정보를 삭제하고 남긴 메시지 확인**(유출 인지)**
		18:00	▸ 웹서버 폐쇄 및 피해 사항 파악, 인터넷망 차단
	11. 26.	-	▸ 운영체제 및 서버 버전 업그레이트, 계정 비밀번호 변경
		15:20	▸ 웹서버 외부 접근포트 차단
	11. 28.	-	▸ 백업DB로 일부 복구, 홈페이지 SSL인증 완료
	11. 30.	18:21	▸ 개인정보 포털에 **유출신고**
	12. 1.	18:14	▸ 개인정보 유출 사실 **홈페이지 공지**(팝업)
2024	1. 10.	-	▸ 정보주체 개인정보 **유출 통지**(이메일)

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’24. 12. 6. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였고, 피심인은 ’24. 12. 20. 개인정보보호위원회에 법 위반사실을 인정하고 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보의 안전성 확보조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

가. 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(대통령령 제33723호, 이하 ‘시행령’) 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.”라고 규정하면서 “개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치(제2호), 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치(제3호), 개인정보를 안전하게 저장 · 전송하는데 필요한 다음 각 목의 조치(제4호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 다음 각 목의 조치(제5호)”를 규정하고 있다.

한편, 위 법령에 따른 안전성 확보 조치에 관한 세부 기준을 정한 「개인정보의 안전성 확보조치 기준」(개인정보위 고시 제2023-6호, 이하 ‘고시’) 제5조제5항은 “개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.” 라고, 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”라고 하면서 “개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가 받지 않은 접근 제한(제1호)”을 규정하고 있다. 또한, 제7조제1항은 “개인정보처리자는 비밀번호, 생체인식 정보 등 인증정보를 저장 또는 정보통신망을 통하여 송 · 수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화 하여야 한다.”라고 규정하고 있으며, 제8조제1항은 “개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관 · 관리하여야 한다.”고 규정하고 있다.

나. 위법성 판단

피심인이 월부터 월까지 개인정보처리시스템(DB)의 취급자 계정에 유추하기 쉬운 비밀번호를 설정한 행위는 보호법 제29조, 시행령 제30조제1항제2호, 고시 제5조제5항 위반에 해당하고,

피심인이 월부터 월까지 개인정보처리시스템(DB)에 접속할 수 있는 권한을 IP 주소 등으로 제한하고, 개인정보에 대한 불법적인 접근 및 유출 시도에 대한 탐지·차단 조치를 취하지 않은 행위는 보호법 제29조, 시행령 제30조제1항제3호, 고시 제6조제1항 위반에 해당하며,

월부터 월까지 정보주체의 비밀번호를 안전하지 않은 암호 알고리즘( )으로 암호화하여 저장하고, 홈페이지 로그인 시 정보통신망을 통해 전송하는 비밀번호를 암호화하지 않고 수신한 행위는 보호법 제29조, 시행령 제30조제1항 제4호, 고시 제7조제1항 위반에 해당한다.

또한, 월부터 월까지 개인정보취급자가 개인정보처리시스템(DB)에 접속하여 처리한 기록을 1년 이상 보관·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제30조 제1항제5호, 고시 제8조제1항 위반에 해당한다.

2. 개인정보 유출 통지 및 신고를 소홀히 한 행위

[보호법 제34조(유출 등의 통지·신고)제1항·제3항]

가. 관련 법 규정

보호법 제34조제1항은 “개인정보처리자는 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 ‘유출등이 된 개인정보 항목(제1호)’, ‘유출등이 된 시점과 그 경위(제2호)’, ‘정보주체가 할 수 있는 방법 등에 관한 정보(제3호)’, ‘개인정보처리자의 대응조치 및 피해 구제절차(제4호)’, ‘정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처(제5호)’를 정보주체에게 알려야 한다.”라고 규정하고 있고,

같은 조 제3항은 “개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

피심인이 개인정보 유출 사실을 인지하였으나 정당한 사유 없이[1] 72시간을 경과하여 홈페이지에 유출 사실을 게시하고, 개인정보 유출을 신고한 행위는 보호법 제34조제1항 및 제3항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준」(개인정보위 고시 제2023-3호, 이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인은 민법 제32조에 따른 비영리 재단법인으로 과징금 부과기준 제6조제3항제1호에 따라 매출액을 산정하지 않고, 법인세법 제4조제3항제1호에 따른 수익사업에서 생기는 소득이 없어 매출액의 산정이 곤란한 경우에 해당하는 바, 보호법 제64조의2제1항 단서 및 같은 법 시행령 제60조의2제2항제1호다목에 따라 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

나. 기준금액

1) 중대성의 판단

보호법 시행령 제60조의2제6항 [별표 1의5] 제2호가목에 따라 과징금 산정 시 기준금액은 위반행위의 내용 및 정도, 암호화 등 안전성 확보 조치 이행 노력, 유출 규모 및 위반행위와의 관련성 등을 종합적으로 고려하여 판단한 위반행위의 중대성에 따라 산정된다. 과징금 부과기준 제8조제1항은 보호법 시행령 [별표 1의5] 제2호가목 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준에 따른다고 규정하고 있다.

---

1) 피심인은 유출 인지 후 전남경찰청 사이버수사대에 신고하고 한국지역정보개발원에 사고신고서를 접수하는 등 피해 확산 방지 등을 위해 노력하였으나 보호법 상의 통지 기한을 엄수하지 못했다고 소명

위 [별표]에 따르면 위반행위의 중대성의 정도는 ① 고의·과실, ② 위반행위의 방법, ③ 위반행위자가 처리하는 개인정보의 유형 및 ④ 위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등 총 네 가지 고려사항별 부과기준을 종합적으로 고려하여 판단하되, 고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과 수준을 적용하여야 한다. 고려사항별로 보면, ① 고의·과실은 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려하여 판단하여야 하고, ② 위반행위의 방법은 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주·대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하여 판단하되, 개인정보가 유출된 경우에는 유출과 안전성 확보조치 위반행위와의 관련성을 포함하여 판단하여야 하며, ③ 개인정보의 유형은 민감정보 또는 고유식별정보인지, 인증정보인지 여부에 따라 판단하고, ④ 정보주체의 피해 규모 및 정보주체에게 미치는 영향은 피해 개인정보의 규모, 위반기간, 정보주체의 권리·이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하여 판단하되, 개인정보가 유출된 경우에는 유출 규모 및 공중에 노출되었는지 여부를 포함하여 판단하여야 한다.

본 유출 사건은 피심인이 개인정보처리시스템(DB)을 운영하면서 접근통제, 암호화 등 3개 이상의 안전조치 의무를 위반하여 개인정보 유출을 초래하였으므로 중대한 과실이 있다고 봄이 타당하며, 위반행위의 부당성도 상당하다. 유출된 개인정보에 민감정보·고유식별정보나 인증정보는 포함되지 않았으며, DB에 보관하고 있던 개인정보 전체가 유출 및 삭제되었다는 점에서 피해 규모 및 정보주체에게 미치는 영향이 적다고 보기 어렵다. 따라서, **위반행위의 중대성을 '중대한 위반행위'로 판단**한다.

2) 기준금액의 산출

보호법 시행령 [별표 1의5] 제2호가목 2)에 따라 과징금 산정 시 기준금액은 위반행위의 중대성에 따라 산정하는바, '중대한 위반행위'의 기준금액은 2억 원 이상 7억 원 미만이며, 피심인의 경우에는 유출 인지 후 지체 없이 취약점을 개선한 한편, 유출된 개인정보가 공중에 노출된 정황은 현재까지 확인되지 않은 점, 조직적 위반이나 내부 관여가 없는 점 등을 참작하여 **그 기준금액을 200,000천 원으로 한다**.

<시행령 [별표 1의5] 2. 가. 2)에 따른 기준금액>

위반행위의 중대성	기준금액
매우 중대한 위반행위	7억 원 이상 18억 원 이하
중대한 위반행위	2억 원 이상 7억 원 미만
보통 위반행위	5천만 원 이상 2억 원 미만
약한 위반행위	5백만 원 이상 5천만 원 미만

다. 1차 조정

피심인은 를 운영하면서 월부터 월까지 접근통제, 암호화 등 3개 이상의 안전조치의무를 소홀히 하여 위반행위의 기간이 2년을 초과하므로 과징금 부과기준 제9조제1항제1호나목에 따라 기준금액의 **100분의 50에 해당하는 100,000천 원을 가산**한다.

아울러, 피심인은 위반행위로 인하여 경제적·비경제적 이득을 취한 사실이 없으므로 과징금 부과기준 같은 조 제2항제1호에 따라 기준금액의 **100분의 30에 해당하는 60,000천 원을 감경**하고, 피심인이 비영리 재단법인이라는 점을 고려하여 같은 항 제2호에 따라 기준금액의 **100분의 50에 해당하는 100,000천 원을 감경**한다.

라. 2차 조정

피심인은 이 사건 유출과 관련된 홈페이지에 접속이 되지 않는 현상을 발견한 웹서버를 폐쇄하고 인터넷망을 차단하는 등 시정 조치하였고, 조사기간 중 일관되게 행위사실을 인정하면서 조사에 적극 협력하였는바, 과징금 부과기준 제10조제2항제1호가목 및 나목의 감경 사유에 해당하므로 같은 조 제3항에 따라 1차 조정을 거친 금액(140,000천 원)의 **100분의 30에 해당하는 42,000천 원을 감경**한다.

마. 과징금의 결정

피심인의 보호법 제29조 위반행위에 대한 과징금은 같은 법 제64조의2제1항제9호, 같은 법 시행령 제60조의2 [별표 1의5] 및 과징금 부과기준에 따라 위와 같이 1차 조정 및 2차 조정을 거쳐 산출한 금액인 **98,000천 원을 최종 과징금**으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•중대한 위반행위 (200,000천 원 적용)	•2년 초과(50% 이내) : 50% 가중(100,000천 원) •취득이익 없음(30% 이내) : 30% 감경(60,000천 원) •비영리재단(50% 이내) : 50% 감경(100,000천 원)	•시정완료 및 조사협력 : 30% 감경(42,000천 원)	**98,000천 원**
⇒ 200,000천 원	⇒ 140,000천 원	⇒ 98,000천 원	

2. 과태료 부과

피심인의 보호법 제34조(개인정보 유출 등의 통지·신고)제1항 및 제3항 위반행위에 대해 같은 법 제75조제2항제17호 및 제18호, 시행령 제63조의 [별표2] 제2호 노목, 도목 및 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 9. 11., 이하 '과태료 부과지침') 에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 보호법 제34조제1항 및 제3항 위반행위에 대해 시행령 제63조 [별표2] 제2호 노목 및 도목에 따라 기준금액을 각각 **1회 위반에 해당하는 600만 원**으로 한다.

< 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
노. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제17호	600	1,200	2,400
도. 법 제34조제3항을 위반하여 보호위원회 또는 전문기관에 신고하지 않은 경우	법 제75조 제2항제18호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

피심인의 보호법 제34조제1항 및 제3항 위반행위는 가중사유에 해당하지 않아 **기준금액을 유지**한다.

2) 과태료의 감경

피심인은 비영리 재단법인인 경우로서 비영리성 등을 고려할 때 과중하다고 인정되는 경우에 해당하여 기준금액의 30%를 감경하고, 조사 기간 중 일관되게 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였고, 사전통지 및 의견 제출 기간 종료일인 '24.12.20. 이전에 시정을 완료하였으므로 과태료 부과지침 제6조에 따라 **기준금액의 100분의 70에 해당하는 420만 원을 각각 감경**한다.

< 과태료 부과지침 [별표 2] - 과태료 감경기준 >

기준	감경사유	감경비율	
업무형태	위반행위자가 비영리법인, 비영리단체 등인 경우로서 무보수성, 공익성, 비영리성 등을 고려할 때 과중하다고 인정되는 경우	기준금액의 30% 이내	최대 50%
조사협조	보호위원회의 조사기간 중 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 20% 이내	최대 50%
자진시정 등	1. 과태료의 사전 통지 및 의견 제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 20% 이내	

다. 최종 과태료

피심인의 보호법 제34조제1항 및 제3항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 **360만 원의 과태료를 부과**한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 유출 통지 위반	600만 원	-	420만 원 (기준금액의 70%)	**180만 원**
개인정보 유출 신고 위반	600만 원	-	420만 원 (기준금액의 70%)	**180만 원**
계				**360만 원**

3. 공표명령

개인정보보호위원회는 보호법 제66조제2항에 따라 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과처분 등을 한 경우 처분 등을 받은 자에게 해당 처분 등을 받았다는 사실을 공표할 것을 명할 수 있다.

피심인의 보호법 제29조 위반행위는 공표지침 제6조제1항제7호(위반행위 시점을 기준으로 위반상태가 3년을 초과하여 지속된 경우)에 해당하며, 위반행위가 인터넷을 통하여 이루어졌으므로 보호법 제66조제2항, 공표 및 공표명령 지침 제8조(공표명령 방법) 및 제11조(인터넷 등 공표)에 따라 피심인에게 처분 등에 대한 통지를 받은 날부터 30일 이내에 당해 처분을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)에 2일 이상 5일 미만의 기간 동안 게시하는 방법으로 공표할 것을 명한다. 이때, 구체적인 공표내용과 방법 등은 개인정보보호위원회와 미리 문서로 협의를 거쳐야 한다.

Ⅵ. 결론

피심인의 보호법 제29조(안전조치의무), 제34조(개인정보 유출 등의 통지·신고)제1항 및 제3항 위반행위에 대하여 같은 법 제64조의2(과징금), 제75조(과태료) 및 제66조(결과의 공표)에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

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

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

과태료 부과 처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과 처분은 「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.

2025년 7월 23일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 김 휘 강 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)