개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-016-235호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 ㈜해성디에스 (사업자등록번호 :)

대표자

의결연월일 2025. 7. 23.

주 문

1. 피심인에 대하여 다음과 같이 과징금을 부과한다.

   가. 과 징 금 : 343,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 법 위반 내용 및 처분 결과를 피심인의 홈페이지에 공표할 것을 명령한다.

   가. 피심인은 처분 등에 대한 통지를 받은 날부터 1개월 이내 당해 처분 등을 받은 사실 등을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만 기간 동안(휴업일 포함) 게시하여야 한다.

나. 피심인은 원칙적으로 표준 공표 문안을 따르되, 공표 문안에 관하여 개인정보보호위원회와 미리 문서로 협의해야 하고, 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 개인정보보호위원회와 협의하여 정하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 반도체 재료의 제조 및 판매업을 영위하면서, 주주 정보, 임직원 정보, 협력사 직원 정보 등의 개인정보를 처리하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 개인정보가 유출된 사실을 인지('24. 6. 3.)하고 유출신고('24. 6. 5.)함에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('24. 6. 21. ~ '25. 6. 13.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 유출 관련 사실관계

1) 유출 경위

신원 미상의 자(이하 '해커')는 피심인이 운영하는 사 의 취약점을 악용하여 VPN에 로그인 후, 프로그램을 통해

1) 법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행

사내망에 접근하였다.

해커는 호스트에 접근한 이후 ~ 사이에 내부 시스템 확인 및 개 시스템 접근 후 데이터를 외부로 유출한 것으로 파악되었다.

이후, 해커는 ~ 기간 중 피심인이 운영하는 다수의 시스템에 랜섬웨어 파일을 배포 및 감염시켰다.

2) (유출 내용) 피심인의 사내망 내 에 저장되어 있던 73,975명의 주주 정보, 임직원 정보, 협력사 직원정보

구분	유출 항목	유출 규모
총 계		73,975명

3) 유출 인지 및 대응

일 시	인지 및 대응 내용
'23. 10. 29. 08:00	시스템 장애 발생 후 서버 전수 확인 결과 랜섬웨어 침해사고 인지
'23. 10. 29. ~ 11.17.	랜섬웨어 감염 경로 조사, 해커 협상에 불응하며 시스템 복구 추진
'24. 06. 03. 12:32	KBS 기자가 피심인에 주주정보 유출 샘플 데이터를 송부하여 개인정보 **유출 인지**
'24. 06. 05. 16:11	개인정보 포털에 **유출 신고**(1차, 51,515명)
'24. 06. 06.	개인정보 유출 정보주체 대상 개인정보 **유출 통지**(이메일, 우편)
'23. 06. 07. ~ 08.16.	홈페이지에 개인정보 유출 사실 팝업 공지

일 시	인지 및 대응 내용
’24. 06. 30.	개인정보 유출 추가 확인
’24. 07. 01. 08:18	개인정보 포털에 **유출 신고**(2차, 22,460명)
’24. 07. 02.	유출 정보주체 대상 개인정보 **유출 통지**(이메일, 문자, 우편)

3. 개인정보의 취급.운영 관련 사실관계

가. 고유식별정보 및 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인이 운영 중이던 장비 제조사인 와 한국인터넷진흥원은 취약점에 대한 조치 안내문을 게재하였으나, 피심인이 주민등록번호 등 개인정보를 처리하면서 해당 취약점에 대한 패치 적용 등 조치하지 아니한 사실이 있다.

또한, 피심인은 ~ 기간 동안 개인정보를 처리하는 일부 시스템에서 악성프로그램을 방지·치료 기능이 동작하지 않은 채로 운영한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 2025. 6. 16. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 7. 4. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

보호법 제24조제3항은 “개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지

아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.”라고 규정하고 있고, 같은 법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속 기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령[2](이하 ‘시행령’) 제21조제1항에서는 “법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다.”라고 규정하고 있고, 같은 영 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위한 ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’를 해야 한다.” 라고 규정하고 있으며, 시행령 제30조제1항제6호는 “개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치를 해야 한다.” 라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준[3]」(이하 ‘고시’) 제6조제3항은 “개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.”라고 규정하고 있고, 제9조제1항은 “개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, ‘프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지(1호)’, ‘발견된 악성프로그램 등에 대해 삭제 등 대응 조치(2호)’의 사항을 준수하여야 한다.”라고 규정하고 있다.

2) 대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행
3) 개인정보보호위원회 고시 제2023-6호, 2023. 9. 22. 시행

2. 위법성 판단

가. 고유식별정보 및 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제24조(고유식별정보의 처리 제한)제3항, 제29조(안전조치의무)]

피심인이 운영 중이던 장비 제조사인 와 한국인터넷진흥원은 취약점에 대한 조치 안내문을 게재하였으나, 피심인이 주민등록번호 등 개인정보를 처리하면서 해당 취약점에 대한 패치 적용 등 조치하지 아니한 행위는 보호법 제24조제3항 및 제29조, 시행령 제21조제1항 및 제30조제1항제3호, 고시 제6조제3항 위반에 해당한다.

또한, 피심인이 ~ 기간 동안 개인정보를 처리하는 일부 시스템에서 악성프로그램을 방지·치료 기능이 동작하지 않은 채로 운영한 행위는 보호법 제24조제3항 및 제29조, 시행령 제21조제1항 및 제30조제1항제6호, 고시 제9조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호법 위반에 대한 과징금 부과기준[4]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과[5]한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항, 시행령 제60조의2에 따라 위반행위가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 초과하지 아니하는 범위에서 부과할 수 있다.

---

4) 개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행

5) 본 건은 랜섬웨어(악성프로그램) 감염으로 개인정보 유출 및 훼손이 동시에 발생한 사건으로, 고시 제9조 위반 행위로 인해 이를 방지하지 못한 경우로 판단하여 보호법 제29조 위반에 대한 과태료를 별도 부과하지 않음

나. 기준금액

1) 중대성의 판단

과징금 부과기준 제8조제1항은 “시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.”라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 “위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단”하고, “고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.”라고 규정하고 있으며, “고려사항별 부과수준의 판단기준은 ▲(고의ㆍ과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 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 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리ㆍ이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.”라고 규정하고 있다.

피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 ’매우 중대한 위반행위‘로 판단한다.

2) 기준금액 산출

피심인은 과징금 부과기준 제6조제3항에 따라 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 결과 산정된 매출액 산정이 곤란한 경우에 해당하고, 시행령 [별표 1의5] 2. 가. 2) 에 따른 '매우 중대한 위반행위'의 해당하여 기준금액을 700,000천 원으로 한다.

<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	7~18억원 이하
중대한 위반행위	2~7억원 미만
보통 위반행위	5천만원~2억원 미만
약한 위반행위	5백만원~5천만원 미만

다. 1차 조정

과징금 부과기준 제9조에 따라 피심인이 위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 기준금액의 100분의 30에 해당하는 금액인 210,000천 원을 감경한다.

라. 2차 조정

과징금 부과기준 제10조에 따라 피심인이 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우, 조사에 적극 협력한 경우 등을 종합적으로 고려하여, 1차 조정을 거친 금액의 100분의 30에 해당하는 금액인 147,000천 원을 감경한다.

마. 부과과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2제1항제9호, 시행령 제60조의2, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 2) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 343,000천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
• 매우 중대한 위반 (기준 금액 700,000천 원)	• 취득이익이 없으므로 30% 감경 (210,000천 원)	• 시정완료, 조사협력을 고려하여 30% 감경 (147,000천 원)	**343,000천 원****
⇒ 700,000천 원	⇒ 490,000천 원	⇒ 343,000천 원	

** 과징금 부과기준 제11조제5항에 따라 1억원 이상인 경우에는 1백만원 단위 미만의 금액을 버림

2. 결과 공표명령

보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침[6]」(이하 '공표 지침') 제6조제1항에 따라 '1천 명 이상 정보주체의 고유식별정보 또는 민감정보를 분실·도난·유출·위조·변조·훼손한 행위로 인하여 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고 또는 과태료 부과 처분을 받은 경우(2호)'에 해당하고 위반행위가 인터넷을 통하여 이루어졌으므로 제8조 및 제11조에 따라 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만의 기간 동안(휴업일 포함) 공표하도록 명한다. 다만, '1일간 다시 보지 않기' 기능의 사용 등 팝업창 설정방식 등은 보호위원회와 협의하여 정한다.

이때 제7조제1항, 제8조제3항에 따라 원칙적으로 공표 지침 [별표]의 표준 공표 문안을 따르되, 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 하고, 제11조제3항에 따라 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

6) 개인정보보호위원회 지침, 2025. 7. 1. 시행

Ⅵ. 결론

피심인의 보호법 제24조(고유식별정보의 처리 제한)제3항 및 제29조(안전조치의무) 위반 행위에 대해서 같은 법 제64조의2(과징금) 및 제66조(결과의 공표)에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

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

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)