개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-013-041호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 이화여자대학교 (사업자등록번호 :)

대표자

의결연월일 2025. 6. 11.

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 같은 시정조치를 명한다.

   가. 피심인은 학사행정정보시스템에 대한 불법적인 접근 및 유출사고 방지를 위하여 모의해킹 등 소스코드 취약점 점검을 강화하고, 비인가 접근이나 유출시도 발생 시 즉각적으로 탐지·대응하는 상시 모니터링 시스템을 구축·운영할 것

   나. 피심인은 주민등록번호 관리 강화 방안을 마련하고 소속 개인정보취급자에

대한 개인정보 보호 교육을 정기적으로 실시할 것

다. 피심인은 가.의 시정조치를 이행하고, 시정명령 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과 또는 계획을 제출할 것

3. 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 5일 이상 7일 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

4. 피심인에 대하여 다음과 같이 징계를 권고한다.

가. 피심인은 본 건 개인정보 유출 및 안전조치의무 위반에 책임이 있는 자(대표자 및 책임있는 임원 포함)를 징계할 것

나. 피심인은 가.의 징계 조치를 이행하고, 징계권고 통보를 받은 날로부터 60일 이내에 그 결과를 개인정보보호위원회에 통보할 것. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 반드시 포함하여 통보할 것

이 유

Ⅰ. 기초 사실

피심인은 「고등교육법」에 따라 설립된 사립대학으로서 「개인정보 보호법」[1](이하 '보호법') 제2조제6호나목 및 같은 법 시행령 제2조제5호에 따른 공공기관에 해당하며, 보호법 제2조제5호에 따른 개인정보처리자로서 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수
이화여자대학교				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출 신고('24.9.6.)에 따라 보호법 위반 여부를 조사하였으며, 그 결과 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 학사 행정 업무를 수행하기 위해 유레카 통합행정시스템(이하 '유레카')을 이용하여 '25. 2. 4. 기준으로 아래와 같이 개인정보를 수집·보유하고 있

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

다.

구 분	수집·이용 항목	수집일	건수(명)

*

※ 피심인은 '15.11.30.부터 유레카 시스템을 통해 학사 관련 개인정보를 처리하고 있음

나. 개인정보 유출 관련 사실관계

1) 유출 경위

신원 미상의 자(이하 '해커')는 '24. 9. 2. 14:50 ~ 9. 3. 11:55 해외 IP에서 유레카 시스템에 존재하는 DB 트랜잭션( ) 기능의 취약점*을 이용하여 파라미터 변조 및 무작위 대입을 통해 졸업생 및 학부생의 개인정보를 조회하였다.

* 로 접근하여 개인정보 조회 시 세션값 검증 로직 부재로 세션값과 조회 대상 정보가 불일치하는 경우에도 파라미터(학번) 변조를 통해 다른 사용자의 개인정보 조회가 가능한 취약점 존재

2) 유출 내용

위 해커의 공격으로 피심인 소속 학부생 및 학부 졸업생 83,352명의 개인정보*가 유출되었다.

* 성명, 학번, 주민등록번호, 국적, 주소, 전화번호, 핸드폰번호, 이메일, 계좌정보, 본

적, 종교, 학적정보, 보호자 정보(성명, 직업, 주소, 전화번호, 핸드폰번호, 본적)

3) 유출 인지 및 대응

일 시		사고 인지 및 대응 내역
'24. 9. 3.	11:50	웹방화벽 로그 모니터링 중 이상행위 탐지
	12:00	공격 의심 IP 차단
	18:16	비인가 접근 시도 시 결과가 조회되지 않도록 소스코드 수정
'24. 9. 5.	11:00	로그 분석 결과 개인정보 유출 사실 **인지**
'24. 9. 6.	11:00	**유출 안내문 홈페이지 게시**, 정보주체에게 **유출 통지**(이메일, 4,472명*)
	11:55	개인정보 **유출 신고**(KISA, 교육부)
'24. 9. 11.		재발 방지를 위한 보안 강화 계획 수립
'24. 10. 21.	13:30	KISA 유출사고 분석 중 비정상 로그 추가 발견
'24. 10. 23.	16:00	2차 **유출 통지**(이메일/SMS,)
'24. 10. 24.	10:00	2차 **유출 신고**(KISA, 교육부)

* 오래 전 수집한 개인정보로 전화번호는 대부분 유효한 연락처가 아니라고 판단하여 이메일주소를 보유한 경우에 한해 이메일로 개별 통지하고, 보충적으로 학교 및 동창회 홈페이지에 유출 안내문 게시

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '25. 3. 21. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '25. 4. 10. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보의 안전성 확보조치를 소홀히 한 행위

[보호법 제24조제3항, 제29조(안전조치의무)]

가. 관련 법 규정

보호법은 개인정보처리자의 안전조치의무에 관하여 제29조에서 “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 있으며, 특히 고유식별정보에 관하여는 같은 법 제24조제3항에서 “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 있다. 이에 따라 보호법 시행령 제30조제1항은 개인정보처리자는 ‘개인정보에 대한 접근을 통제하기 위한 조치(제3호)’를 하여야 한다고 규정하면서, 같은 영 제21조에서 “법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다”라고 규정하고 있다.

한편, 위 법령에 따른 안전성 확보 조치에 관한 세부 기준을 정한「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호, 이하 ‘고시’) 제6조1항은 “정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도를 탐지 및 대응(제2호)’하는 등의 안전조치를 하여야”하고, 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 있다.

나. 위법성 판단

피심인이 등의 보안장비 구축 및 비정상적인 속도로 반복 호출 시 해당 IP를 차단하는 등의 기본적인 보안체계는 갖추고 있었으나,

하는 것과 같은 이상행위에 대한 탐지·대응 기준 부재 등 피심인의 시스템 이용 환경을 분석하여 적절한 탐지·차단 기준을 수립·적용하는 것을 소홀히 하였으며, 특히 자체 관제 인력이나 외부 서비스 등을 이용한 모니터링이 이루어지지 않는 야간 및 주말에는 이 사건 유출 사고와 같은 다양한 형태의 이상행위를 탐지하여 즉각 대응할 수 있는 체계가 미흡하여 '24. 9. 2. ~ 9. 3. 사이 발생한 해킹 공격을 적시에 차단하지 못한 것은 접근통제 조치를 소홀히 한 행위로서 보호법 제24조제3항 및 제29조, 시행령 제21조제1항 및 제30조제1항제3호가목, 고시 제6조제1항을 위반한 것이다.

또한, 피심인이 유레카 시스템을 구축·운영하면서 개인정보 조회 시 세션값과 조회 대상 정보가 불일치하는 경우에도 파라미터 변조를 통해 다른 사용자의 개인정보가 조회되는 취약점이 존재함에도 이를 장기간 방치한 것은 보호법 제24조제3항 및 제29조, 시행령 제21조제1항 및 제30조제1항제3호다목, 고시 제6조제3항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 보호법 제24조(고유식별정보의 처리 제한)제3항 및 제29조(안전조치의무) 위반행위에 대하여 같은 법 제64조의2제1항제9호, 시행령 제60조의2제6항 [별표 1의5] 및 「개인정보 보호법 위반에 대한 과징금 부과기준」(개인정보보호위원회고시 제2023-3호, 2023. 9. 15. 제정·시행, 이하 '과징금 부과기준')에 따라 다음과 같이 과징금을 부과한다.

가. 과징금 상한액

피심인은 보호법 제2조제6호나목 및 시행령 제2조제5호에 따른 공공기관(국립

대학)으로서 본 건 유출과 관련된 위반행위는 수익사업과 무관한 학사 행정 업무 영역에서 발생하였으므로 매출액이 없거나 매출액의 산정이 곤란한 경우에 해당하는바, 보호법 제64조의2제1항 단서 및 같은 법 시행령 제60조의2제2항제1호다목에 따라 20억 원을 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.

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, 정보주

체의 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 시스템의 취약점을 악용한 외부 공격으로 인해 개인정보가 유출된 것으로서, 피심인이 등 기본적인 보안장비를 구축·운영하였던 점으로 보아 피심인에게 위반의 고의가 있다고 보기는 어려우나, 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근통제 조치를 철저히 하여야 함에도 주말이나 야간에는 시스템을 통한 탐지 이외에 탐지된 내용을 확인하고 즉시 차단 등의 적절한 조치를 이행하는 것을 소홀히 하여 위 공격에 제대로 대응하지 못한 결과 대규모의 개인정보 유출을 초래하였으므로 중대한 과실이 있다고 봄이 타당하며, 유레카 시스템의 DB 트랜잭션 취약점을 장기간 보완하지 않음으로써 개인정보 유출이 초래되었다는 점에서 위반행위의 부당성도 상당하다. 이로 인해 83,352명의 개인정보가 유출되었고, 특히 유출 항목에 주민등록번호 등 고유식별정보 및 계좌번호와 같은 중요한 정보가 포함되어 있다는 점에서 피해규모 및 정보주체에게 피해를 입힐 가능성이 매우 크다고 할 것이다. 따라서 위반행위의 중대성을 '매우 중대한 위반행위'로 판단한다.

2) 기준금액 산출

보호법 시행령 [별표 1의5] 제2호가목 2)에 따라 과징금 산정 시 기준금액은 위반행위의 중대성에 따라 산정하는바, '매우 중대한 위반행위'의 기준금액은 7억 원 이상 18억 원 이하이며, 피심인의 경우에는 일정 속도 이상의 반복 호출에 대한 IP 차단 등 기본적인 탐지·대응 기준은 수립되어 있었던 점, 일과시간 중에는 모니터링을 하고 있었던 점, 이를 통해 해킹 도중 이상행위를 탐지하여 즉시 IP를 차단함으로써 추가 유출을 막는 한편, 취약점 관련 소스코드 수정 등 개선조치를 이행한 점, 그 밖에 개인정보 보호책임자를 지정하였으며 내부의 조직적 위반 정황이 없는 점 등을 참작하여 그 기준금액을 700,000천 원으로 한다.

<시행령 [별표 1의5] 2. 가. 2)에 따른 기준금액>

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

다. 1차 조정

피심인은 유레카 시스템이 구축된 '15. 11. 30.부터 '24. 9. 3.까지 유레카에 존재하는 세션 검증 취약점에 대한 조치를 취하지 않고 비인가 접근 제한 및 유출 탐지·대응 등 접근통제 조치를 소홀히 하여 위반행위의 기간이 2년을 초과하므로 과징금 부과기준 제9조제1항제1호나목에 따라 기준금액의 100분의 50에 해당하는 350,000천 원을 가산한다. 아울러, 피심인은 이 사건 위반행위로 인하여 경제적 또는 비경제적 이득을 취한 사실이 없으므로 같은 조 제2항제1호에 따라 기준금액의 100분의 30에 해당하는 210,000천 원을 감경하고, 피심인 대학의 재학생 수 등 기관 규모 및 재정 여건을 종합적으로 고려하여 같은 항 제2호에 따라 기준금액의 100분의 50에 해당하는 350,000천 원을 감경한다.

라. 2차 조정

피심인은 이 사건 유출과 관련된 이상 징후를 발견한 '24. 9. 3. 공격 의심 IP를 차단하고, 비인가 접근 시도 시 결과가 조회되지 않도록 소스코드를 수정하는 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(490,000천 원)의 100분의 30에 해당하는 147,000천 원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제24조제3항 및 제29조 위반에 대한 과징금은 같은 법 제64조의2 제1항제9호, 같은 법 시행령 제60조의2 [별표 1의5] 및 과징금 부과기준에 따라 위와 같이 1차 조정 및 2차 조정을 거쳐 산출한 금액인 343,000천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
•매우 중대한 위반행위 (700,000천 원 적용)	•위반기간 2년 초과 : 50% 가산 (350,000천 원) •취득이익 없음: 30% 감경 (210,000천 원) •업무형태 및 규모: 50% 감경 (350,000천 원)	•시정완료 및 조사협력 : 30% 감경 (147,000천 원)	**343,000천 원**
⇒ 700,000천 원	⇒ 490,000천 원	⇒ 343,000천 원	

2. 시정명령

피심인이 이 사건 유출의 직접적인 원인에 해당하는 유레카 시스템의 세션 검증 취약점은 개선 조치하였으나, 인력 및 예산 부족 등의 사유로 현재와 같이 관제가 제대로 이루어지지 않는다면 향후에도 주말이나 야간 등 취약한 시간대에 유출 시도가 발생할 경우 즉각 대응이 어려울 것으로 판단되는바, 피심인에게 보호법 제64조제1항에 따라 주문 제2항과 같이 시정조치할 것을 명한다.

3. 공표명령

개인정보보호위원회는 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(보호법 제66조제2항).

피심인의 보호법 제24조제3항 및 제29조 위반행위는「개인정보 보호법 위반

에 대한 공표 및 공표명령 지침」(개인정보보호위원회 지침, 2023. 10. 11. 시행, 이하 '공표 및 공표명령 지침') 제6조제1항제2호(1천 명 이상 정보주체의 고유식별정보를 유출한 행위로 인하여 시정조치 명령 및 과징금 부과 처분을 받은 경우), 제3호(위반행위가 보호법 제64조의2제1항제9호에 해당하여 과징금을 부과받은 경우로서 영 [별표 1의5] 제2호가목에 따른 위반행위의 중대성의 정도가 '매우 중대한 위반행위'에 해당하는 경우) 및 제7호(위반행위 시점을 기준으로 위반상태가 3년을 초과하여 지속된 경우)에 해당하고, 위반행위가 인터넷을 통하여 이루어졌으므로 보호법 제66조제2항, 공표 및 공표명령 지침 제8조 및 제11조에 따라 피심인에게 처분 등에 대한 통지를 받은 날부터 30일 이내에 당해 처분을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)에 5일 이상 7일 미만의 기간 동안 게시하는 방법으로 공표할 것을 명한다. 이때, 구체적인 공표내용과 방법 등은 개인정보보호위원회와 미리 문서로 협의를 거쳐야 한다.

4. 징계권고

개인정보보호위원회는 보호법 제65조제2항에 따라 개인정보 보호와 관련된 법규의 위반행위가 있는 경우 대표자 및 책임있는 임원을 포함하여 그 위반행위에 책임이 있는 자를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다.

피심인은 학적부 작성·관리 등 교육의 과정 기록에 관한 사무를 수행하기 위하여 당사자의 동의 여부와 관계 없이 학생의 개인정보를 주민등록번호 등 고유식별정보를 포함하여 광범위하게 처리하는 개인정보처리자의 지위에 있어 개인정보가 유출되지 않도록 더욱 철저히 안전성 확보에 필요한 조치를 해야 함에도 유레카 시스템의 세션 검증 취약점을 시스템 구축 시부터 9년 가까이 인지·개선하지 못하였고, 각종 보안장비 구축 및 일부 악성 공격에 대한 IP 자동 차단 등 기본적인 보안 체계는 갖추고 있었으나, 다양한 형태의 외부 공격을 탐지하여 즉각 대응할 수 있는 모니터링 체계가 다소 미흡하였으며, 인력 및 예산 부족 등을 이유로 일과시간 외에는 외부의 불법적인 접근이나 유출 시도에 대한 탐지·대응을 게을리 하여 본건 유출사고에 이르게 되었다. 이에 보호법 제65조제2항 및 「개인정보 보호 법규 위반에 대한 징계권고 기준」(개인정보보호위원회 지침, 2023. 10. 11. 시행, 이하 '징계

권고지침') 제3조제1항제3호(위반행위가 보호법 제64조의2제1항제9호에 해당하여 과징금을 부과받은 경우로서 영 [별표 1의5] 제2호가목에 따른 위반행위의 중대성의 정도가 '매우 중대한 위반행위'에 해당하는 경우) 및 제4호(위반행위의 대상이 된 개인정보가 고유식별정보로서 정보주체의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 경우)에 따라 본 건 유출 및 안전조치의무 위반에 책임이 있는 자를 징계할 것을 권고한다.

피심인은 징계권고 통지를 받은 날로부터 60일 이내에 그 결과를 개인정보보호위원회에 통보하여야 하며, 권고를 따르지 않을 경우 그 사유를 반드시 명시하여 통보하여야 한다.

Ⅴ. 결론

피심인의 보호법 제24조제3항 및 제29조(안전조치의무) 위반행위에 대하여 같은 법 제64조의2(과징금의 부과) 제1항제9호, 제64조(시정조치 등)제1항, 제65조(고발 및 징계권고)제2항, 제66조(결과의 공표)제2항에 따라 과징금 부과, 시정명령, 공표명령 및 징계권고를 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.

이상과 같은 이유로 주문과 같이 의결한다.

2025년 6월 11일

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)