개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-013-094호 (사건번호 : 2021조총0071)

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인

의결연월일 2022. 8. 10.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 고등교육법에 따른 공공기관으로「개인정보 보호법 시행령」 제2조 5호에 따른 개인정보처리자이다.

< 피심인의 일반현황 >

사업자 등록번호 (법인등록번호)	대표자 성명	주소	직원 수

※ 자료 출처 : 피심인 제출자료

Ⅱ. 사실조사 결과

1. 행위 사실

개인정보보호위원회[1]는 개인정보 유출신고 건과 관련하여 피심인의「개인정보 보호법」위반 여부에 대한 사실조사('21. 6. 9. ~ '22. 5. 27.) 결과, 다음과 같은 사실을 확인하였다.

가. 개인정보 수집·이용 현황

○ 피심인은 강의에 따른 지원금 제공을 위해 개발도상국 교수 1,909명의 개인정보(성명, 주민등록번호, 연락처 등)를 수집하여 보유하고 있음

1) 2020. 8. 5. 시행된 개정「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관 사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

구분	항목	수집일	건수
회원 정보	(필수) 이름 , 아이디, 비밀번호, 성별, 생년월일, 이메일, 직업, 국가, 소속기관, 직책, 전공, 닉네임	'11. 6. 21 ~ '21. 9. 17.	1,909

나. 개인정보 유출 관련 사실관계

○ 미상의 헤커가 피심인이 운영하고 있는 ‘ 홈페이지’를 SQL 인젝션 공격하여 회원 정보 탈취 및 다크웹 게시

* 공격자가 주소창 또는 ID·PW 창에 SQL명령어를 입력한 후 웹사이트에 침투 서버를 제어하고, 해당 서버가 공격명령어에 따라 데이터베이스 정보를 출력하는 방식

○ 개인정보 유출 경과 및 대응

- '21. 9. 27. 15:00 피심인은 교육부 사이버안전센터로부터 침해사고 분석 보고서를 통보받고 유출사실 인지
- '21. 9. 29. 18:04 정보주체에게 유출통지(이메일)
- '21. 9. 29. 18:45 홈페이지에 유출 사실 게재
- '21. 9. 30. 11:05 한국인터넷진흥원에 개인정보 유출 신고

※ 피심인은 **00**국제개발협력원에서 유지보수업체 없이 홈페이지를 운영하다가 유출 사고가 의심된다는 통보를 받고 2021. 9. 24.부터 홈페이지 서비스 및 관리자 페이지를 폐쇄조치 함

○ 유출 규모 및 항목

- 개발도상국 교수 1,909명*의 개인정보

* 개발도상국(우즈베키스탄 등 14개국) 교수들의 개인정보(중복가입자 포함)

구분	유출 항목(개발도상국 교수들의 개인정보)
필수	이름, 아이디, 비밀번호, 전화번호, 성별, 생년월일, 이메일, 직업, 국가, 소속기관, 직책, 전공, 닉네임

다. 개인정보 보호법규 위반 행위 사실

1) 개인정보의 안전성 확보조치를 소홀히 한 행위

○ 피심인은 개인정보의 안전성 확보조치 기준(행정안전부 고시 제2019-47호, 2019.6.7.)개정에 따라 접속기록의 보관기관 및 점검시기[2] 등에 중요한 변경이 있음에도 내부 관리 계획에 이를 즉시 반영하지 않은 사실이 있으며,

- 또한, '유네스코 유니스트윈 홈페이지' DB에서 개인정보취급자 및 회원의 비밀번호를 안전한 암호알고리즘으로 암호화하지 않은 사실이 있다.

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 4. 5. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2022. 4. 20. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 위법성 판단

가. 개인정보처리자는 개인정보의 안전성 확보조치 기준에 규정된 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 하나

- 피심인이 내부관리계획에 접속기록 변경사항을 반영하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제4조제3항을 위반한 것이다.

---

2) '개인정보의 안전성 확보조치 기준' 개정(2019.6.7.)으로 접속기록 보관기관이 최소 6개월에서 1년으로 변경되었으며 접속기록의 점검 시기도 반기별 1회에서 월 1회로 변경되었으나 피심인은 이를 내부관리계획에 반영하지 아니하였음

나. 개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 하나

- 피심인이 ‘ 홈페이지’ DB에서 개인정보취급자 및 회원의 비밀번호를 안전한 암호알고리즘으로 암호화하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제7조제5항을 위반한 것이다.

2. 관련 법 규정

***「개인정보 보호법」 제29조(안전조치의무)**

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.

***「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치)**

① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

*** 개인정보의 안전성 확보 조치 기준(고시)**

제4조(내부 관리계획의 수립·시행)

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정절차를 통하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립·시행하여야 한다.

7. 접속기록의 보관 및 점검에 관한 사항

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제7조(개인정보의 암호화)

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대한 과태료는 같은 법 제75조제2항제6호,

같은 법 시행령 제63조의〔별표2〕「과태료의 부과기준」에 따라 다음과 같이 부과한다

가. 기준금액

개인정보보호법 시행령 과태료부과기준(제63조 관련) 개인정보 수집 이용 위반, 안전조치의무 위반에 대한 과태료는 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 과태료 금액 600만원을 적용한다.

< 과태료 부과기준 > (단위 : 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27, 개인정보위, 이하 '과태료 부과지침') 제8조 [별표2] 가중 기준에 따라 위반행위별 각 목의 세부 기준에서 정한 행위가 2개에 해당하므로 기준금액의 10%를 가중한다.

<과태료의 가중기준>

기준	가중 사유	가중비율
위반의 정도	2. 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30%이내

다. 과태료 감경

'과태료 부과지침' 제7조 [별표1] 감경기준에 따라 과태료의 사전통지 및 의견 제출 기간 내에 위반행위를 중지하는 등 시정을 완료함에 따라 기준금액의 50%인 300만원을 감경한다.

<과태료의 감경기준>

기준	감경사유	감경비율
조사 협조 · 자진 시정 등	1. 과태료의 사전통지 및 의견 제출 기간이 종료되기 이전에 위반 행위를 중지하는 등 시정을 완료한 경우	기준금액의 50%이내

※ 과태료 부과지침 제7조(과태료의 감경기준)에 따라 과태료의 감경은 기준금액의 50%을 초과할 수 없음

라. 최종 과태료

기준금액에 가중 및 감경사유를 적용한 360만원의 과태료를 부과한다.

< 최종 과태료 산출내역(안) >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	위반내용	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
법 §29	안전조치 의무 위반	600	60	300	**360**

☞ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진 납부 하는 경우, 100분의 20을 감경함(질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제75조(과태료) 제2항제6호에 따라 과태료 부과를 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.