개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-009-056호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 5. 25

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 13,500,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은「고등교육법」 제2조 제4호에 따른 전문대학이자「개인정보 보호법」(법률 제14839호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보 처리자이며, 일반현황은 다음과 같다.

< 피심인 일반현황 >

대표	설립일자	상시직원 수	매출액('20년)	주요서비스

Ⅱ. 사실조사 결과

개인정보보호위원회[1]는 피심인의 개인정보 유출신고 건과 관련하여 「개인정보 보호법」 위반 여부에 대한 사실조사( ) 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 사고 경위 및 규모

'19년도 7월, 는 침입탐지시스템을 통해 명의 개인정보가 유출된 것을 확인하고 에 통지하였다. 홈페이지의 게시판 파일 업로드 기능을 이용하여 웹셸* 및 에스큐엘 인젝션** 공격을 받아 개인정보가 유출되었으며, 유출된 개인정보 항목은 학번, 성명, 주민등록번호, 비밀번호, 이메일주소, 휴대전화번호였으며, 주민등록번호의 암호화 여부는 시스템 로그에 기록되지 않았다.

* 웹쉘(Web Shell) : 시스템에 명령을 내릴 수 있는 코드로서, 웹서버 취약점을 통해 서버 스크립트가 업로드되면 해커들은 보안 시스템을 통해 별도 인증 없이 시스템에 접속 가능하여 원격으로 해당 웹서버를 조종할 수 있음

** SQL 인젝션(Structed Query Language Injection) : 데이터베이스에 대한 질의값을 조작해 해커가 원하는 자료를 데이터베이스로부터 유출하는 공격 기법

1) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 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)

는 해킹 기법상 웹셸로 인해 최대 명(중복 제외시 명)의 개인정보가 유출되었을 것이라고 추정하였으나, 개인정보보호위원회(당시는 행정안전부) 점검 결과 개인정보처리시스템에 유출(다운로드) 관련 로그가 없어 명 외에 유출 증적은 확인하지 못하였다.

나. 사고인지 및 대응

○ **('19.7.16.)** 에서 피심인에 유출사실 통지

○ **('19.7.17.)** 에서 통지받은 공격지 IP차단

○ **('19.7.18~19.)** 에서 침해사고 분석 후 추가 조치

- 추가 공격자IP 차단, 확인된 악성파일 삭제, 관리자페이지 접근통제, 게시판 업로드 기능 삭제 등

○ **('19.7.22.)** 개인정보보호위원회(당시는 행정안전부)에 유출신고

○ **('19.7.23)** 홈페이지에 유출공고 및 이메일주소가 있는 정보주체 명에게 유출통지

- **('19.7.25)** 추가로 반송된 이메일(명)과 이메일 주소가 없는 정보주체(명)에게 문자로 2차 통지
- **('19.7.26)** 주소만 있는 정보주체(명)와 재반송된 이메일 발송자에게 우편통지

2. 개인정보보호 법규 위반 행위 사실

가. 보관기간이 지난 개인정보를 파기하지 않은 행위

피심인은 시스템에서 퇴직 후 5년 이상 경과자('19.7.31. 기준 명)의 주민등록번호를 파기하지 않고 보관한 사실이 있다.

나. 주민등록번호를 안전하게 보관하지 않은 행위

피심인은 시스템에서 일부 테이블의 주민등록번호를 평문으로 보관한 사실이 있다.

다. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 시스템과 시스템에 대해 연 1회 이상 내부 관리계획의 이행 실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 시스템에서 비밀번호를 암호화하지 않고 평문으로 전송한 사실이 있다.

3) 피심인은 시스템과 시스템에서 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '개인정보보호법 위반 기관에 대한 행정처분 등 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 위반 사실을 인정하고 위반사항에 대해 전부 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 보관기간이 지난 개인정보를 파기하지 않은 행위

가. 관련법 규정

보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”고 규정하고 있다.

「국세기본법」 제85조의3 제1항은 “납세자는 각 세법에서 규정하는 바에 따라 모든 거래에 관한 장부 및 증거서류를 성실하게 작성하여 갖춰 두어야 한다.” 고 규정하고 있으며, 2항에서 “제1항에 따른 장부 및 증거서류는 그 거래사실이 속하는 과세기간에 대한 해당 국세의 법정신고기한이 지난 날부터 5년간 보존하여야 한다.” 라고 규정하고 있다.

나. 위법성 판단

피심인이 학사행정종합 정보관리 시스템에서 퇴직 후 5년 이상이 경과한 자의 주민등록번호를 파기하지 않은 행위는 보호법 제21조 제1항을 위반한 것이다.

2. 주민등록번호를 안전하게 보관하지 않은 행위

가. 관련법 규정

보호법 제24조의2제2항은 “개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다”고 규정하고 있다.

나. 위법성 판단

피심인이 에서 주민등록번호를 저장할 시

일부 테이블에서 암호화하지 않은 행위는 보호법 제24조의2 제2항을 위반한 것이다.

3. 개인정보에 대한 안전조치의무를 소홀히 한 행위

가. 관련법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행(제1호), 개인정보를 안전하게 저장·전송할 수 있는 암호화기술의 적용 또는 이에 상응하는 조치(제3호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하도록 규정하고 있으며,

시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인「개인정보의 안전성 확보조치 기준(행정안전부고시 제2019-47호)」에서 개인정보처리자의 안전성 확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

① 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리하여야 한다 (제4조제4항)

② 개인정보처리자는 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에

는 이를 암호화하여야 한다. (제7조제1항)

③ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하며, 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다. (제8조제2항)

나. 위법성 판단

피심인이 ① 에서 개인정보보호 내부관리 계획의 이행 실태를 연 1회 이상 점검·관리하지 않은 사실(고시 제4조제4항), ② 에서 비밀번호를 암호화하지 않고 평문으로 전송한 사실(고시 제7조제1항), ③ 에서 개인정보처리시스템의 접속기록을 월 1회 이상 점검·관리하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」 제29조를 위반한 것이다.

Ⅳ. 처분 및 결정

가. 과태료 부과

피심인의 보호법 제21조(개인정보의 파기)제1항 위반행위에 따라 같은법 제75조제2항제4호 및 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 450만원의 과태료를 부과한다.

피심인의 보호법 제24조의2(고유식별정보의 처리 제한)제2항 위반행위에 따라 같은법 제75조제4항제1호 및 같은 법 시행령 제63조의 [별표2] 「과태

료 부과기준」에 따라 450만원의 과태료를 부과한다.

피심인의 보호법 제29조(안전조치의무) 위반행위에 따라 같은법 제75조제2항제6호 및 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 450만원의 과태료를 부과한다.

1) 기준금액

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 총 1,800만원을 적용한다.

< 과태료 기준금액, 개인정보보호법 시행령 제63조 [별표 2] >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(단위:만원)		
		1회	2회	3회 이상
마. 법 제21조제1항을 위반하여 개인정보를 파기하지 않은 경우	법 제75조 제2항제4호	**600**	1,200	1,800
차. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4호의3	**600**	1,200	1,800
타. 법 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	**600**	1,200	2,400
합계		**1,800**		

나. 과태료의 가중·감경

사전통지 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정한 점을 고려하여 아래와 같이 감경 사유가 인정되어 과태료 부과기준에 따라 기준금액의 25%인 450만원을 감경한다.

< 과태료 부과기준(행정안전부 기준('19.10.7.))>

유형	내용	기준
대상규모	중·소기업	감경(50%)
내용.정도	경미사항 3/10 미만 위반*	감경(50%)
	중요사항 7/10 이상 위반*	가중(50%)
위반자유형	장애/심신미약자 등	감경(50%)
태도.노력	부주의등 + 피해없음	감경(50%)
	검사 전 시정/해소	감경(50%)
	의견제출 기간 시정/해소	감경(25%)
	은폐·조작 위반	가중(50%)
	검사 거부/미시정	가중(50%)
결과	피해자 10만명 이상	가중(50%)
	2차 피해 발생	가중(50%)
	3개월 이상	가중(50%)
기타 필요 시	기타 필요 시	감경
	기타 필요 시	가중

* 과태료 5천만원(75조1항) 적용 조항은 중요사항, 1천만원(75조3항) 적용 조항은 경미사항으로 구분

※ 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되 기준금액의 100분의 50을 초과할 수 없음

다. 최종 과태료

피심인의 개인정보 보호법 위반 사항에 대하여 총 1,350만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제21조제1항, 제24조의2제2항 및 제29조 위반 행위에 대하여 같은 법 제75조(과태료) 제2항에 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 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2022년 5월 25일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)