개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-009-059호

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 : 4,500,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 대학교의 산학협력단으로, 「개인정보 보호법」(법률 제14839호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보 처리자이며, 일반현황은 다음과 같다.

< 피심인 일반현황 >

대표	설립 일자	직원 수	매출액('20년 기준)	주요서비스

Ⅱ. 사실조사 결과

개인정보보호위원회[1]는 월 개인정보보호 포털에 유출신고가 접수된 건과 관련하여 현장조사( ) 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 사고 경위 및 규모

피심인은 운영하고 있는 홈페이지의 관리자페이지( )에 대한 접근 권한을 설정하지 않아 권한이 없는 자에게 월부터 개인정보를 유출하게 한 사실이 있다.

접속기록 분석 결과 총 명( )의 개인정보가 유출된 것으로 확인되었다.

교직원의 경우 이름, 교번, 학과, 직급, 연락처, 이메일 항목이 유출되었고 학생의 경우 이름, 학번, 학과, 학년, 이메일, 재적상태 항목이 유출되었다.

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)

나. 사고인지 및 대응

○ **('20.6.15.)** 민원인이 인터넷진흥원에 유출 제보

* 유출 URL:

○ **('20.6.19.)** 인터넷진흥원에서 피심인에 유출사실 알림(10:29)

- 해당페이지에 관리자만 접근이 가능하도록 인증 적용(13:00)

○ **('20.6.19. ~ 6.22.)** 로그 분석을 통한 유출규모 인지

○ **('20.6.23.)** 행정안전부에 유출신고 및 정보주체에게 개인정보 유출사항 통지

2. 개인정보보호 법규 위반 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보처리시스템(　　)에 대해 연 1회 이상 내부 관리계획의 이행실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 개인정보처리시스템(　　)에 대하여 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리 시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 하나 그러하지 아니한 사실이 있다.

3) 피심인은 개인정보처리시스템(　　)에 대하여 외부에서 관리자페이지에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

4) 피심인은 개인정보처리시스템(　　)에서 인터넷 홈페에지 등을 통하여 열람권한이 없는 자에게 개인정보가 공개되거나 유출되지 않도록 조치를 취하여야 하나 그러하지 않은 사실이 있다.

5) 피심인은 개인정보처리시스템(　　)에서 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 기술적 조치를 취하여야 하나 그러하지 않은 사실이 있다.

6) 피심인은 개인정보처리시스템(　　)에 접속한 기록을 월 1회 이상 점검하여야 하나 그러하지 아니한 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. 안전성 확보에 필요한 조치를 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), 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), 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 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리하여야 한다. (제4조제4항)

② 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. (제5조제6항)

③ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다. (제6조제3항)

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침

해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다. (제6조제5항)

⑥ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다. (제8조제2항)

나. 위법성 판단

피심인이 ①개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ② 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ③ 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6호 제2항) ④ 개인정보처리스템에서 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 사실(고시 제6호 제3항) ⑤ 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 기술적 조치를 취하지 않은 사실(고시 제6조제5항) ⑥ 개인정보처리시스템의 접속기록을 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

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

가. 기준금액 산정

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 총 600만원을 적용한다.

< [별표 2] 과태료의 부과기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(단위:만원)		
		1회	2회	3회 이상
타. 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·감경

사전통지 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정한 점을 고려하여 아래와 같이 감경 사유가 인정되어 과태료 부과기준에 따라 기준금액의 25%인 150만원을 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%)

유형	내용	기준
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 450만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제75조(과태료) 제2항 제6호에 의한 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.

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)