개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-013-092호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 8. 10.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 고등교육법에 따른 대학교로 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

사업자 등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

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.

1. 행위 사실

가. 개인정보 수집 · 이용 현황

피심인은 0000시스템( )을 운영하면서, 가상대학 수강생 관리를 목적으로 '21. 6. 18. 기준 아래와 같이 개인정보를 수집·보유하고 있다.

구분	항목	수집일	건수
이용자(수강생) 정보	(필수) 아이디, 이름, 이메일, 휴대전화번호, 학번, 소속, 성적, 출결	2018. 1 ~ 2021. 6	228,733

※ 0000시스템 實사용자수('21.6.18. 기준 로그인 이력이 있는 사용자) : 50,371명

나. 개인정보 유출 경위

1) 유출경위

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)

피심인의 0000시스템 고도화 전환을 위한 시스템 내 데이터베이스(DB) 이관작업 중 이관항목에 ID를 포함시키지 않아 원 데이터가 정상적으로 이관되지 않았고, 개인의 메시지함에서 타인의 메시지(메시지 제목, 내용, 발송자 성명 등)가 랜덤하게 노출되는 장애가 발생하였다.

◈ 사고 발생시점('21.2.2. 00:00~'05:20) 메시지함 클릭자는 433명으로 확인되었으나, 정확한 유출규모는 특정 불가함(어떤 메시지를 누가 봤는지에 대한 로그기록이 존재하지 않음)

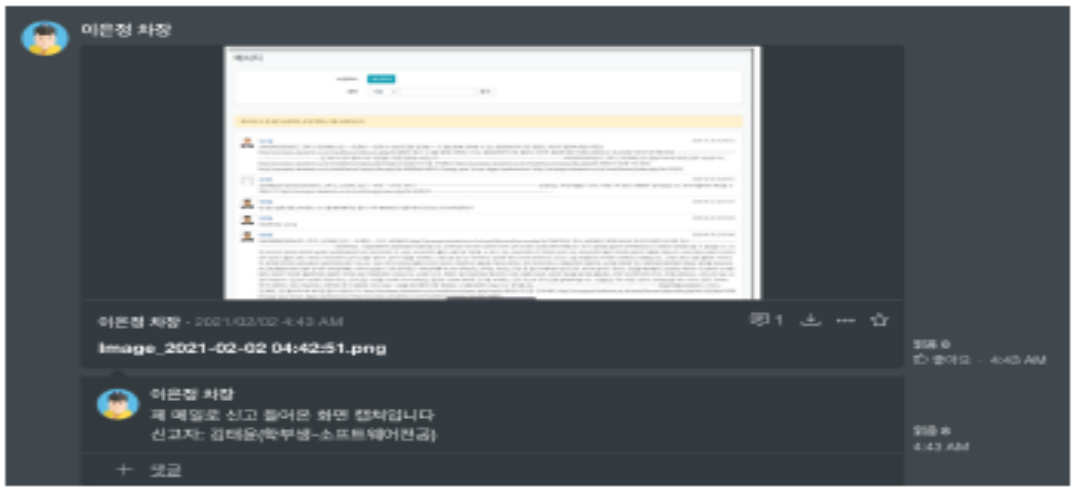
2) 유출경과 및 대응

고도화 작업후 시스템 오픈 (DB 이관)	⇒	(장애 인지) 학부생 **신고**	⇒	(대응·수정) **메시지함**(웹,앱) 기능 등 **중단**	⇒	(분석·검토) 열람자 **로그** 등 **확인** 및 **처리 검토**	⇒	(신고·통지) 유출신고 및 개별**통지·공지**
~ '21. 2. 2.		2.2. 04:25		2.2. 05:20		2.2 09:00~2.4.		2.4. 17:45~2.6.

- ('21.2.2. 00:00) 0000시스템 고도화작업 완료 후 시스템 오픈

  ※ 데이터 이관 오류에 따른 타인의 메시지함 노출

- ('21.2.2. 04:45) 학부생의 신고로 메시지함 장애 사항 인지



이후 에브리타임 서비스 내 장애가 공유된 상황 파악

- ('21.2.2. 05:20) API[2] 기능 중단 및 메시지함 기능 중단
- ('21.2.2. 09:00 ~ '21.2.4.) 메시지함 열람자 로그 확인
- ('21.2.4. 17:45) 0000시스템 내 공지사항 게시
- ('21.2.5. 15:35) 메시지함 열람자 안내 진행(2차 피해방지 관련)
- ('21.2.5. 16:50) 대상자(학생, 교수) 개별 통지 진행

※ 유출통지(1·2차): 433명('21.2.5,이메일), 433명('21.2.5,문자·SNS)
※ 유출통지(3·4차)*: 22,803명('21.2.5, 이메일), 21,067명('21.2.5,문자·SNS)
* '21. 2. 5. 당시 0000시스템 가입 이용자 전체 대상 통지

- ('21.2.6. 14:55) 개인정보보호포털에 개인정보 유출 신고

다. 개인정보 보호법규 위반 행위사실

1) 개인정보에 대한 안전성 확보조치를 소홀히 한 행위

피심인은 0000시스템 고도화를 위한 DB 이관작업시 이관항목에 ID를 포함하지 않아 로그인한 사용자의 메시지함에 타인의 저장 메시지 내용이 표시되게 한 사실이 있다.

2) Application Programming Interface : 컴퓨터와 컴퓨터프로그램 사이의 연결로서 SW인터페이스이며, 컴퓨터와 인간을 연결시키는 사용자 인터페이스와 별개로 컴퓨터와 소프트웨어를 연결하는 인터페이스

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 6. 17. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2022. 7. 1. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 한다고 규정하고 있다.

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 '개인정보에 대한 접근통제 및 접근권한의 제한 조치(제2호)' 등의 안전성 확보조치를 하여야 한다고 규정하고 있다.

같은 법 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 '고시') 제6조제3항은 취급 중인 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 접근통제 등에 관한 조치를 취하여야 한다고 규정하고 있으며, 고시 해설서는 고시 제6조제3항에 대해 인터넷 홈페이지의 설계·개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 취급 중인 개인정보가 노출되지 않도록 필요한 조치를 하여야 한다고 해설하고 있다.

2. 위법성 판단

가. 개인정보의 대한 안전성 확보조치를 소홀히 한 행위

피심인이 0000시스템 DB 이관작업 중 이관항목에 ID를 포함시키지 않아 로그인 한 개인의 메시지함에 타인의 저장 메시지 내용이 표시되게 한 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제6조제3항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 보호조치 위반(접근통제)	보호법 §29	§30①	권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§6③)

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조(안전조치 의무) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호 및 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 부과한다.

가. 기준금액

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

위반행위	근거 법조문	과태료 금액(만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중·감경

1) (과태료의 가중) 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회 지침 '21. 1. 27. 제정, 이하 '과태료 부과지침') 제8조(과태료의 가중)는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 동 지침 [별표2]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중)에 해당하지 않아 가중 없이 기준금액을 유지한다.

2) (과태료의 감경) 과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 동 지침 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제7조(과태료 감경)에 따라 의견제출 기간 내 법규 위반행위를 시정 완료하고, 자료제출 등 조사에 적극 협력한 점을 고려하여 기준 금액의 50%인 300만원을 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

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

다. 최종 과태료

피심인의 개인정보 보호법 제29조를 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 300만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 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.