개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2022-005-025호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 3. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 6,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 영국 대학 진학 예비과정 등을 운영하는 기업으로「개인정보 보호법」(법률 제16930호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	설립일자	자산('20년)	매출액('20년)	주요서비스	종업원 수

피심인은 ①시스템 개발·유지보수 업무를 에 위탁하고, ② 과정 운영 및 관리 업무를 에 위탁하였다.

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021.9월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 시스템을 통해 유학 준비생 명의 개인정보를 수집하였다.

2. 개인정보 유출 경위

가. 사고 경위 및 유출 규모

신원미상의 자가 미상의 방법으로 학생과 학부모의 개인정보를 탈취하여 유학 준비생(명)의 학부모 대상으로 보이스피싱을 하였고, 시스템에서 유학 준비생(최대 명)의 개인정보가 유출되었을 것으로 추정되나, 구체적 유출 경로 및 데이터 확인이 불가하였다.

나. 경과 및 대응

- ’21.9.17. 피심인은 보이스피싱 전화를 받았다는 민원이 지속적으로 제기되어 개인정보가 외부로 유출됨을 의심
- ’21.9.17. 개인정보 유출 통지(문자메시지 및 전화)
- ’21.9.23. 개인정보보호 포털에 유출 신고 및 기술적 안전조치 시행

3. 개인정보보호 법규 위반 행위 사실

가. 개인정보의 안전성 확보를 소홀히 한 행위

1) 피심인은 개인정보취급자(이하 '취급자'라 함)의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않았다.

2) 피심인은 취급자 별로 사용자계정을 발급하지 않고 관리자페이지 계정 1개를 수탁사 직원 5명이 공유하게 하였다.

3) 피심인은 관리자페이지에서 취급자의 비밀번호 설정시 안전한 비밀번호 작성규칙을 적용하지 않았다.

4) 피심인은 관리자페이지에서 취급자의 비밀번호 저장시, 양방향 암호화 알고리즘인 을 사용하여 적용하였다.

5) 피심인은 취급자가 시스템에 접속하여 수행한 업무내역을 알 수 있는 접속기록을 1년 이상 보관·관리하지 않았다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.12.15. 피심인의 의견을 요청하였으며, 피심인은 2021.12.29.에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보의 안전성 확보를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있다.

같은 법 시행령 제30조제1항에서는 개인정보처리자는 법 제29조에 따라 개인

정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호), 개인정보 침해 사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하도록 규정하고 있고,

시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인「개인정보의 안전성 확보조치 기준」(고시 제2020-2호) 제5조제3항은 “개인정보처리자는 개인정보처리시스템에 대한 접근 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야” 하고, 제5조제4항은 “개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야” 하고, 제5조제5항은 “개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야” 하고, 제7조제2항은 “비밀번호 및 생체인식정보는 암호화하여 저장하여야 하며, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야” 하고, 제8조제1항은 “개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다”라고 규정하고 있다.

나. 위법성 판단

피심인이 개인정보취급자 비밀번호를 양방향 암호화 알고리즘을 사용하여 저장하는 등 개인정보처리시스템의 안전성 확보에 필요한 조치를 다 하지 않은 것은 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 [별표2]「과태료의 부과기준」에 따라 다음과 같이 600만원의 과태료를 부과한다.

가. 기준금액

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

< 과태료 부과기준 2. 개별기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
계		600		

나. 과태료의 가중

피심인의 제29조에 따른 안전성 확보에 필요한 조치 위반행위의 정도가 중대하여 과태료의 부과기준에 따라 기준금액(600만원)의 50%인 300만원을 가중한다.

* ①개인정보취급자의 접근권한 부여·변경·말소 내역 미보관, ②사용자계정 1개를 다수의 개인정보취급자와 공유하여 사용, ③개인정보취급자 비밀번호 설정시 안전한 비밀번호 작성규칙 미적용, ④비밀번호 일방향 암호화 저장 미조치, ⑤접속기록 미보관

다. 과태료의 감경

피심인이 사전통지 의견제출 기간 종료 전 위반상태를 모두 시정한 점, 조사기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 적극 협력한 점,「중소기업기본법」제2조에 따른 중기업인 점 등을 고려하여 기준금액(600만원)의 50%인 300만원을 감경한다.

라. 최종 과태료

피심인이 보호법 제29조를 위반한 행위에 대해 600만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

위반조항	위반내용	과태료 금액 (단위 : 만원)			
		기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §29	안전성 확보에 필요한 조치를 하지 않음	600	300	△300	600

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호에 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 3월 23일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　강 정 화　(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 홍 열　(서 명)

위　　원　　지 성 우　(서 명)