개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-009-054호

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 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 「개인정보보호법」(법률 제16930호, ‘이하 “보호법”이라 함) 제2조제5항에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인 일반현황 >

대표자	설립 일자	직원 수	자본금('20년 기준)	주요서비스

Ⅱ. 사실조사 결과

개인정보보호위원회[1]는 '2021. 9월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 보호법 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('21. 12. 13.~12. 15.) 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 유출 경위 및 규모

피심인은 '21.9.2 ~ 9.5 불상의 해커로부터 SQL 인젝션* 공격을 받아 홈페이지 및 홈페이지 DB에 저장되어 있던 개인정보가 유출되었다.

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

접속기록 분석 결과 건의 개인정보가 유출된 것으로 확인되었으며, 은 ID, 비밀번호, 이름, 주소, 집전화번호, 핸드폰번호, 이메일 항목이 유출되었고, 는 ID, 비밀번호, 이름, 생년월일, 주소, 집전화번호, 핸드폰번호, 이메일 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. 유출인지 및 대응

○ **('21. 9. 6~9.13.)** 교육부 사이버안전센터(이하 'ECSC')로부터 홈페이지 침해 관련 자료 제출을 요청받아 자료 분석 및 회신

○ **('21.9.15.)** 개인정보 유출 인지(ECSC 침해사고 분석결과서 수신)

○ **('21.9.16.~9.17.)** 유출된 개인정보 주체에게 개별 문자 및 이메일 통지, 해당 홈페이지 접속차단 및 임시 게시판 오픈, 데이터 백업 후 운영 서버 데이터 삭제

○ **('21.9.17. 20:18)** 개인정보보호 포털에 개인정보 유출 신고

○ **('21.9.23~9.30.)** 개인정보 유출 관련 안내문 홈페이지 공지(팝업) 게시

○ **('21.10.6 14:00)** ECSC에 해당 웹사이트 취약점 점검신청

2. 개인정보보호 법규 위반 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보처리시스템에서 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하였어야 하나, 그러하지 아니한 사실이 있다.

2) 피심인은 개인정보처리자로서 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화하여 저장하여야 하나 그러하지 아니한 사실*이 있다.

* 비밀번호를 평문으로 저장하거나 양방향 알고리즘(ARIA)을 사용하여 암호화함

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 4.21.~2022. 5.10. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2022. 5. 10. 위반 사실을 인정하고 위반사항에 대해 전부 시정을 완료하였다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다”라고 규정하고 있다.

1) 같은 법 시행령 제30조제1항은 안전성 확보조치로 ①개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행, ②개인정보에 대한 접근통제 및 접근 권한의 제한 조치, ③개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치, ④개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치, ⑤개인정보 보안프로그램의 설치·갱신, ⑥개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치를 하도록 하고 있다.

2) 같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’라 함)에서는 다음과 같이 규정하고 있다.

① 개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.(고시 제6조제3항)

② 개인정보처리자는 비밀번호는 암호화하여 저장하여야 하고 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.(고시 제7조제2항)

나. 위법성 판단

피심인이 ①취급중인 개인정보가 개인정보처리스템에서 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 사실(고시 제6호 제3항) ②비밀번호는 암호화하여 저장하여야 하고 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하지 않은 사실(고시 제 7조 2항)은 보호법 제29조를 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 따라 같은 법 제75조제2항 제6호 및 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 360만 원의 과태료를 부과한다.

가. 기준금액

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

< 과태료 부과기준, 개인정보보호법 시행령 제63조 [별표 2] >

(단위 : 만원)

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

나. 과태료의 가중

피심인의 위반행위*는 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상에 해당되어 기준금액의 10%인 60만 원을 가중한다.

* ① 취급중인 개인정보가 개인정보처리시스템에서 인터넷 홈페이지 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 점, ② 접속기록 등을 월1회 이상 점검하지 않은 점

다. 과태료의 감경

피심인이 위반행위에 대하여 사전통지 및 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정을 완료한 점, 조사 기간 중 행위사실을 인정하면서 자료 제출·진술 등 조사에 적극 협력한 점 등을 고려하여 기준금액의 50%인 300만 원을 감경한다.

라. 최종 과태료

피심인의 개인정보 보호법 위반사항에 대하여 총 360만 원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B+C)
제29조(안전성확보 조치 의무 위반)	법 제75조제2항제6호	600	60	△300	**360**

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 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 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)