개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2022-005-019호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 3. 23.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 4,800,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 화재안전 컨설팅 서비스를 제공하면서 개인정보를 처리하는 자로서 「개인정보 보호법」(법률 제16930호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보처리자의 지위를 가지며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	설립일자	매출액('20년)	당기순이익('20년)	종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021.11월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 유출 경과 및 대응

일시		인지 및 대응
'21.11.16.	12:18	신원 미상자가 해외 IP(영국)로 홈페이지에 접근하여 취약점을 탐색하고, 발견한 웹취약점(SQL Injection 취약점)을 악용하여 DB에 저장된 개인정보 탈취를 시작함
'21.11.16.	21:33	신원 미상자가 다크웹에서 계정 판매글을 게시함
'21.11.17.	13:36	농협은행으로부터 다크웹에서 판매되는 개인정보가 피심인의 회원정보로 파악된다는 연락을 수신함
'21.11.17.	13:51	피심인은 홈페이지를 폐쇄 조치함
'21.11.17.	15:18	한국인터넷진흥원이 다크웹에 판매되는 개인정보가 피심인의 회원정보가 맞는지 확인을 요청함
'21.11.17.	16:07	피심인은 홈페이지의 회원정보와 일치한다고 판단하여 개인정보 유출을 신고함
'21.11.28.	00:57	유출의 원인이라고 추정되는 웹 취약점과 관련하여 웹페이지를 수정 조치함
'21.11.17. ~ 12.15.		개인정보 유출 사실을 통지함(이메일, 문자, 유선 등)

나. 유출 규모 및 경위

피심인의 홈페이지 아이피가 과거 농협은행이 사용하던 웹페이지(cyberedu.nonghyup.com)의 아이피였는데, 농협은행이 도메인을 폐기하지 않아 외부에서 cyberedu.nonghyup.com을 입력하면 피심인의 홈페이지로 연결되는 상황이었다. 신원 미상자도 농협은행 개인정보라고 판매하는 것으로 보아 농협은행 웹페이지로 오해한 것으로 추정되고, 웹 취약점을 이용하여 총 회에 걸쳐 DB에 불법적으로 접근하였다. 이를 통해 홈페이지 DB에서 성명, 아이디, 이메일, 비밀번호 등 개인정보가 유출된 것으로 추정된다.

피심인은 웹 취약점으로 악용된 회원가입 웹페이지를 수정하고 관리자 비밀번호에 비밀번호 작성규칙을 적용하였으며, 저장하고 있는 비밀번호를 안전한 암호 알고리즘으로 암호화하는 등의 조치를 하였다. 또한 홈페이지는 폐쇄 조치한 상태이며 향후 서버를 이전하고 취약점을 보완해 새로운 홈페이지를 운영할 예정이다.

2. 개인정보보호 법규 위반 행위 사실

가. 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 관리자(admin) 비밀번호를 숫자 8자리로만 구성하고, 개인정보처리시스템에 접속한 IP주소를 분석해 불법적인 개인정보 유출 시도의 탐지 및 접근제한·차단 등 적절한 대응조치를 하지 못하고 약 번의 접근을 허용하였다.

또한, 비밀번호를 안전한 암호 알고리즘으로 암호화하여 저장하지 않고 취약한 암호화 방식을 사용하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.1.17. ‘개인정보보호 법규 위반에 대한 행정처분 사전통지‘ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 2022.1.21. 피심인은 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 유출 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있고,

같은 법 시행령 제30조제1항은 개인정보처리자는 보호법 제29조에 따라 제2호 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 제3호개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치를 하여야 한다고 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(고시 제2020-2호) 제5조제5항은 “개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하여야”하고, 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응 조치를 해야”하고, 제7조제5항은 “개인정보처리자는 개인정보를 암호화하는 경우 안전한 알고리즘으로 암호화하여 저장하여야 한다”라고 규정하고 있다.

나. 위법성 판단

피심인이 안전한 비밀번호 작성규칙을 관리자 비밀번호 설정에 적용하지 않고, 정보통신망을 통한 불법적인 접근을 탐지하여 제한·차단하지 못한 것과 안전하지 않은 암호화 방식으로 비밀번호를 암호화하여 저장한 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 480만원의 과태료를 부과한다.

가. 기준금액 산정

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

< 과태료 부과기준 >

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 기준금액의 30%인 180만원을 가중한다.

* ①개인정보에 대한 접근 통제 및 접근권한 제한 미조치, ②개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 미흡

다. 과태료의 감경

피심인이 위반행위에 대하여 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료하였고 중소기업기본법에 따른 소기업에 해당하여 기준금액의 50%인 300만원을 감경한다.

라. 최종 과태료

피심인이 보호법 제29조를 위반한 행위에 대해 480만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	처분조항	기준 금액(A)	가중액 (B)	감경액 (C)	**최종액 (D=A+B+C)**
제29조	제75조제2항제6호	600	180	△300	**480**

Ⅴ. 결론

피심인이 보호법 제29조(안전조치의무)를 위반한 행위에 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 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)