개 인 정 보 보 호 위 원 회

심의・의결

안건번호 제2022-005-020호

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 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 고객(회원)의 개인정보를 처리하는 「개인정보보호법」(이하 “보호법”이라 함) 제2조제5호에 따른 개인정보처리자로서 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대표자	개업일자	주요서비스	종업원 수	자산('21년도)

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021. 7월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 개인정보처리시스템을 운영하면서 고객(회원)의 개인정보를 수집·보관하였다.

< 개인정보 수집 현황 >

구 분	항 목	수집기간	건수
회원 정보	(필수) 이름, 아이디, 비밀번호 (선택) 이메일, 성별, 생년월일, 전화번호, 휴대폰번호, 주소	'05년 8월 ~'21년 7월	

2. 개인정보 유출 경위

가. 유출 경위 및 규모

신원 미상자(홍콩 IP)가 홈페이지 취약점을 이용하여 해킹 공격(웹쉘, WebShell)[1]을 통해 서버에 접근, 관리자페이지에 접속 후 회원에게 광고성 스팸 메일을 발송하여 회원의 이메일 주소 건(중복 포함)이 유출되었다.

나. 유출 경과 및 대응

- '21.7.3. 신원 미상자(홍콩 IP)가 홈페이지 관리자페이지에 접근하여 회원 정보를 조회하고, 관리자페이지의 메일보내기 기능을 이용하여 회원들에게 광고성 스팸메일(건)을 발송

※ '20.8.13. 01:44 최초 신원미상자(중국 IP)가 알 수 없는 경로로 웹쉘 파일을 업로드하였으며, 이후 다수의 외부 IP가 동일한 행위로 접근한 이력이 발견됨('20.10.17.~'21.4.20.)

1) 웹쉘(Web Shell)은 시스템에 명령을 내릴 수 있는 코드로서, 간단한 서버 스크립트로 만드는 방법이 널리 사용되고 있으며 웹서버 취약점을 통해 스크립트가 업로드되면 해커들은 보안 시스템을 피해 별도 인증 없이 시스템에 접속 가능하여 원격으로 해당 웹서버를 조종할 수 있음

※ 보안 관제업체()에서 모니터링 중 웹쉘이 탐지되었으며, 다량의 메일 발송 및 발송 대기 중인 메일(여건)이 확인되어 즉시 삭제 조치

- ’21.7.3. 업무담당자는 사내 관계자들과 정보를 공유하며 다른 직원으로부터 광고성 스팸메일 수신 제보를 받음

- ’21.7.5. 내부 회의(광고성 스팸메일 발송) 및 업무 보고 후 홈페이지 유지보수업체에 스팸메일 수신자 이메일 주소 분석 및 추출 의뢰

- ’21.7.6. 개인정보(이메일 주소) 유출 사실 인지 후 신고·통지(이메일)

- ’21.7.13. 안정적인 홈페이지의 운영을 위해 호스팅 서비스 업체 변경

- ’21.7.14. 관할 수사기관에 신고

3. 개인정보보호 법규 위반 행위 사실

가. 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

신원 미상자(홍콩 IP)가 알 수 없는 경로로 피심인의 개인정보처리시스템에 접근하였으며, 관리자페이지의 메일보내기 기능을 통해 회원들에게 광고성 메일을 발송한 사실이 확인되었다.

이와 관련하여, 피심인은 호스팅 서비스 업체가 제공하는 솔루션 기능을 통해 개인정보처리시스템에 대한 접속 권한을 특정 IP주소로 일부 제한하는 조치는 하였으나, 인가하지 않은 외부 IP주소의 적절한 차단 조치는 하지 않았다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.2.7. ‘개인정보 보호법 위반기관 행정처분 사전통지’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 개인정보보호위원회에 선처를 요청하였다.

Ⅲ. 위법성 판단

1. 개인정보처리시스템의 안전성 확보 조치를 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.

1) 같은 법 시행령 제30조제1항에서는 개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)의 안전성 확보 조치를 하도록 규정하고 있다.

2) 시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(위원회 고시)」에서 개인정보처리자의 안전성 확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

가) 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호), 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(제2호)의 기능을 포함한 조치를 하여야 한다.(고시 제6조제1항)

나. 위법성 판단

피심인은 개인정보처리시스템에 접속한 IP주소를 분석해 불법적인 개인정보 유출 시도를 탐지하고 접근제한·차단 등 적절한 대응조치를 하지 않은 피심인의 행위는 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 300만원의 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 위반행위는 과태료 부과기준 1. 일반기준 라.에 규정된 가중할 수 있는 사유에 해당하는 사항이 없으므로 가중 없이 기준금액을 유지한다.

다. 과태료의 감경

피심인은 「중소기업기본법」 제2조에 따른 중기업으로, 조사기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 협력한 점 등을 고려하여 과태료 부과기준에 따라 기준금액의 50%인 300만원을 감경한다.

라. 최종 과태료

피심인의 제29조 위반 행위에 대해 기준금액 600만원에서 50%를 감경한 300만원을 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**
계		600	-	△300	**300**

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호에 의한 과태료를 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　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)