개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2022-005-016호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 Fluke Corporation
6920 Seaway Blvd., Everett, WA 98203, United States

의결연월일 2022. 3. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 9,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위에 따른 행정처분의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 오프라인 대리점을 통해 산업계측기를 판매하는 자로서 「舊개인정보 보호법」(법률 제14839호, 이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대표자	주소	설립일자
	6920 Seaway Blvd., Everett, WA 98203, United States	1953.10.7.

Ⅱ. 사실조사 결과

1. 개인정보 유출 경위

가. 유출 경로 및 규모

'18년 Fluke 직원이 실수로 개인 GitHub에 관리자 암호키(AWS Access Key)가 포함된 소스코드를 게시하면서 코드가 공개적으로 접근이 가능해졌고, '20.6.10. Fluke GitHub 계정에 올려진 소스코드 접근 서비스를 제공하던 WayDev社의 보안 침해 사고로 Fluke Connect 소스코드가 유출되었다. 신원 미상자가 알 수 없는 방법으로 AWS 구성에 접근을 허용하는 AWS Access Key를 탈취하여 신원 미상자가 '20.6.23. 해외 IP(네덜란드)로 AWS에 접근하였으며, '20.6.26. Fluke Connect 계정에 해외 IP로 접근하여 악성 시스템을 생성하고, 자국 IP로 접근하여 새로운 AWS 관리자 계정을 생성하였다. 이를 통해 한국 이용자 명의 개인정보(성명, 회사명, 이메일 주소, 연락처 등)가 유출되었다.

피심인은 FBI 수사와 자체 조사 결과 신원 미상자가 사용한 IP주소가 동일한 점 등 Fluke Connect 침해사건과 WayDev 보안 침해 사건 간의 관련성이 발견되었다고 소명하였다.

피심인은 WS Access Key를 교체하고 공용 계정이 아닌 개인 계정의 소스 코드에 암호키가 저장되지 않도록 규정을 명문화하였으며, Fluke Connect 계정 보호를 위해 로그인 시에 다중 인증을 적용하고 모든 관리자 Key에 대하여 VPN을 연결하여 사용하고 있다.

나. 경과 및 대응

일시	인지 및 대응
'20. 6. 26.	의심스러운 활동이 발생하였다는 알림 메일 수신
'20. 6. 27.	Fluke Connect AWS 계정의 모든 접근을 차단
'20. 6. 29.	기술지원팀이 신원 미상자로부터 Fluke DB에 대한 금전 요구 이메일을 수신하고 개인정보 유출 사실을 인지
'20. 7. 2.	외부 분석업체를 고용해 포렌식 조사를 실시
'20. 7. 14.	한국 이용자 명에게 이메일 통지
'20. 7. 21.	개인정보보호 포털에 유출 신고

2. 행위 사실

가. 개인정보에 대한 접근통제를 소홀히 한 행위

피심인은 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하지 않아, 신원 미상자가 탈취한 AWS Access Key로 데이터베이스에 무단 접근하여 개인정보가 유출되었다.

나. 개인정보 유출 신고를 지연한 행위

피심인은 '20.6.26. 의심스러운 활동을 감지하고 '20.6.29. 개인정보 유출 사실을 인지하였으나, '20.7.14. 한국 이용자에게 통지하고 개인정보보호 포털에 '20.7.21. 신고하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.10.6. 피심인의 의견을 요청하였으며, 2021.10.19. 피심인은 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보에 대한 접근통제를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 유출되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 해야 한다고 규정하고 있다.

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다고 규정하고 있고, 제2호는 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치를 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(행안부 고시, ‘19.6.7.) 제6조제2항은 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다고 규정하고 있다.

나. 위법성 판단

외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하여야 하나 이를 하지 않아 개인정보가 유출된 피심인의 행위는 보호법 제29조 위반에 해당한다.

2. 개인정보 유출 신고를 지연한 행위

가. 관련 법령의 규정

보호법 제34조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 알려야 하고, 제3항은 대통령령으로 정한 규모 이상(1천명 이상)의 개인정보가 유출된 경우에는 지체 없이 전문기관에 신고하여야 한다고 규정하고 있다.

나. 위법성 판단

개인정보 유출 사실을 안 때에는 지체 없이(5일 이내) 이용자에게 알리고 한국인터넷진흥원에 신고하여야 하나, 15일이 지나서 통지·신고한 피심인의 행위는 보호법 제34조제1항 및 제3항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 및 제34조제1항·제3항 위반에 대해 같은 법 제75조제2항 및 시행령 제63조 [별표2]에 따라 900만원의 과태료를 부과한다.

가. 기준금액 산정

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

< 과태료의 부과기준 >

위반행위	근거 법조문	위반횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
타. 법 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1200	2400
어. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1200	2400
저. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조 제2항제9호	600	1200	2400
계		1,800		

나. 과태료의 가중

피심인의 각 위반행위에 대하여 과태료 부과기준에 따른 가중사유는 없으므로 기준금액을 유지한다.

다. 과태료의 감경

피심인의 각 위반행위에 대하여 위법 결과를 검사 이전 및 의견제출 기간 전에 시정 또는 해소하였으므로 기준금액의 50%인 300만원을 각각 감경한다.

라. 최종 금액

피심인의 보호법 제29조, 제34조제1항 및 3항 위반에 대하여 기준금액 1,800만원에서 900만원을 감경하여 총 900만원의 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	-	△300	**300**
제34조제1항	제75조제2항제8호	600	-	△300	**300**
제34조제3항	제75조제2항제9호	600		△300	**300**
합 계		1,800	-	△900	**900**

2. 결과 공표

피심인의 위반행위가 개인정보 보호법 제66조 및 같은 법 시행령 제61조에 해당하므로 피심인의 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

「(舊)개인정보 보호법」 위반 행정처분 결과 공표

(舊)개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용

2022년 0월 00일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인이 보호법 제29조, 제34조제1항 및 제34조제3항을 위반한 행위에 대하여 같은 법 제75조제2항에 의한 과태료 부과, 현행 개인정보 보호법 제66조에 의한 공표를 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 흥 열　(서 명)

위　　원　　지 성 우　(서 명)