개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2022-005-014호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 Canva PTY Ltd.
110 Kippax St., Surry Hills, NSW 2010, Australia

의결연월일 2022. 3. 23.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

   가. 피심인은 개인정보처리시스템에 허용되지 않은 접근이 발생하지 않도록 적절히 관리하는 등 재발 방지 대책을 마련할 것

   나. 위 가의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출할 것

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 10,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 피심인의 일반 현황

피심인은 영리를 목적으로 정보통신망을 통해 디자인 서비스를 제공하는 자로서 舊정보통신망이용 촉진 및 정보보호 등에 관한 법률(법률 제16021호, 이하 “정보통신망법”이라 함) 제2조제1항제3호에 따른 정보통신서비스 제공자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표 자	주 소	설립일자
	110 Kippax St., Surry Hills, NSW 2010, Australia	2012.6.12.

Ⅱ. 사실조사 결과

1. 개인정보 유출 경위

가. 유출 경로 및 규모

개발자가 테스트 목적으로 생성한 Buildkite 프로그램의 소스코드에 개인정보처리시스템에 접근할 수 있는 AWS Access Key가 저장되어 있었고, 신원 미상자가 ’19.5.18. Buildkite의 취약점을 이용해 크리덴셜 스터핑*(Credential Stuffing) 공격을 시도하였고, ‘19.5.24. Buildkite 접속에 성공하여 시스템 접속 정보 및 AWS Access Key를 탈취하고 이용자 데이터베이스에 무단 접속하였다. 이를 통해 한국 이용자 최대 명의 개인정보(계정정보, 이름, 국가, 이메일 주소, 도시, 결제정보 등)가 유출되었다.

* 크리덴셜 스터핑 : 다른 곳에서 유출된 아이디·비밀번호 등의 로그인 정보를 무작위로 대입하여 로그인하는 수법

피심인은 개발자 등이 Buildkite에 접속할 때 모든 계정에 대해서 ID/PW와 추가적 2차 인증을 의무화하였으나, Buildkite를 API로 접속하는 경우 2차 인증을 우회할 수 있는 취약점이 존재하였다고 소명하였다.

피심인은 Buildkite社에 취약점 존재 사실을 신고하고 개선 요청, AWS Access Key를 통한 무단 접근 방지를 위해 IP 접근통제, 2차 인증 강화 및 Key 발급 절차를 강화하였고, 소스코드 내 AWS Access Key 등의 접근 정보가 저장되지 않도록 주기적인 모니터링을 실시하고 관리 강화 프로세스를 도입하였다.

나. 경과 및 대응

일시		인지 및 대응
‘19. 5. 25.	00:45	시스템 모니터링 과정 중 침입 사실을 탐지
‘19. 5. 25.	04:30	개인정보 유출 사실을 인지
‘19. 5. 25.	21:41	웹사이트에 유출 사실 공지, 영어 이용자에게 통지
‘19. 5. 27.	00:28	한국어 이용자에게 통지
‘19. 6. 13.		개인정보보호 포털에 개인정보 유출신고

2. 행위 사실

가. 개인정보에 대한 접근통제를 소홀히 한 행위

피심인은 외부에서 이용자 데이터베이스(DB)에 접속하려는 경우 안전한 인증 수단을 적용하지 않아, 신원 미상자가 탈취한 AWS Access Key로 데이터베이스에 무단 접근하여 개인정보가 유출되었다.

나. 개인정보 유출 신고를 지연한 행위

피심인은 ’19.5.25. 시스템 침입 사실을 탐지하고 개인정보 유출 사실을 인지하였으나 ’19.6.13. 개인정보 유출을 신고하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.7.20. ’개인정보보호 법규 위반에 대한 행정처분 사전통지‘ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 2021.10.14. 피심인은 의견을 제출하였다. 이에 개인정보보호위원회는 라고 검토하였다.

Ⅲ. 위법성 판단

1. 개인정보에 대한 접근통제를 소홀히 한 행위

가. 관련 법령의 규정

정보통신망법 제28조제1항은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 유출을 방지하고 개인정보의 안전성을 확보하기 위하여 다음 각 호의 기술적·관리적 조치를 하여야 하고, 그 중 제2호는 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 규정하고 있다.

같은 법 시행령 제15조제2항은 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다고 규정하고 있고, 제1호는 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행을 규정하고 있다.

「(舊)개인정보의 기술적·관리적 보호조치 기준」(방통위 고시, ‘15.5.19.) 제4조제4항은 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다고 규정하고 있다.

나. 위법성 판단

외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하여야 하나 피심인이 이를 적용하지 않아 개인정보가 유출된 것은 정보통신망법 제28조제1항 위반에 해당한다.

2. 개인정보 유출 신고를 지연한 행위

가. 관련 법령의 규정

정보통신망법 제27조의3제1항은 정보통신 서비스 제공자등은 개인정보의 유출 사실을 안 때 지체 없이 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 신고해서는 아니 된다고 규정하고 있다.

나. 위법성 판단

개인정보 유출 사실을 안 때에는 지체 없이(24시간 이내) 한국인터넷진흥원에 신고하여야 하나 피심인이 24시간을 경과하여 신고한 피심인의 행위는 정보통신망법 제27조의3제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과징금 미부과

「(舊)개인정보 보호 법규 위반에 대한 과징금 부과기준」(방통위 고시 '15.8.27.) 제9조는 위반행위가 경미하여 시정조치로 갈음할 수 있는 경우 과징금 부과 대신 시정명령을 할 수 있도록 규정하고 있다.

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 산정액은 소액으로서 과징금 부과의 실효성이 크지 않은 경우에 해당하므로 과징금에 갈음하여 시정을 명한다.

2. 시정명령

피심인에게 정보통신망법 제64조제4항에 따라 위반행위의 시정을 위하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보처리시스템에 허용되지 않은 접근이 발생하지 않도록 적절히 관리하는 등 재발 방지 대책을 마련할 것

나. 위 가의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출할 것

3. 과태료 부과

피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반에 대해 같은 법 제76조제1항 및 시행령 제74조 [별표9]에 따라 1,000만원의 과태료를 부과한다.

가. 기준금액 산정

피심인이 최근 3년간 같은 각 위반행위로 과태료 처분을 받은 사실이 없으므로 2개의 위반행위에 대해 기준금액은 1회 위반에 해당하는 1,000만원을 각각 적용한다.

< 과태료의 부과기준 >

위반행위	근거 법조문	위반횟수별 과태료금액(만원)		
		1회	2회	3회 이상
하. 법 제27조의3제1항을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조제1항 제2호의3	1,000	2,000	3,000
너. 법 제28조제1항에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조제1항 제3호	1,000	2,000	3,000
계		2,000		

나. 과태료의 가중

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

다. 과태료의 감경

피심인은 각 위반행위에 대해 사전 통지 기간 전에 시정을 완료하고 조사기간 중 일관되게 행위사실을 인정하면서 조사에 적극 협력하였으며 위반행위의 정도나 동기 등을 고려하여 기준금액의 50%인 500만원을 각각 감경한다.

라. 최종 금액

피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반에 대하여 기준금액 총 2,000만원에서 1,000만원을 감경하여 1,000만원의 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)**
제27조의3제1항	제76조제1항제2호의3	1,000	-	△500	**500**
제28조제1항	제76조제1항제3호	1,000	-	△500	**500**
합 계		2,000	-	△1,000	**1,000**

4. 결과 공표

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

「(舊)정보통신망 이용촉진 및 정보보호 등에 관한 법률」 위반 행정처분 결과 공표

(舊)정보통신망 이용촉진 및 정보보호 등에 관한 법률 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 월 일
개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인이 정보통신망법 제27조의3제1항 및 제28조제1항을 위반한 행위에 대하여 같은 법 제76조제1항에 의한 과태료 부과, 정보통신망법 제64조제4항에 의한 시정조치, 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)