CLOUDFLARE

백서

데이터 개인정보 보호 및 법 집행 요청에 대한 Cloudflare의 정책

게시일: 2021년 1월 28일

개요

Cloudflare의 네트워크 및 사업은 궁극적으로 고객의 신뢰를 바탕으로 구축됩니다. Cloudflare는 Cloudflare 시스템의 보안을 개선하고 보관 중이거나 이동 중인 데이터를 암호화하며 고객이 세계의 다양한 지역에서 트래픽을 검사하는 방법을 결정하도록 제품을 개발하고 배포함으로써 신뢰를 얻고 유지합니다.

하지만 공학적인 방법으로 모든 문제를 해결할 수 있는 것은 아닙니다. 따라서 Cloudflare는 Cloudflare 시스템에 있는 고객 및 최종 사용자의 데이터를 관리하는 방법과 데이터에 대한 정부 및 기타 법적 요청에 대응하는 방법에 대한 정책 및 절차도 유지합니다.

이 백서에서는 이러한 정책을 개괄적으로 설명하고 데이터 개인정보 보호 및 규제 준수에 대한 Cloudflare 접근법의 다양한 측면을 자세하게 다룬 링크를 제시합니다. 그 내용은 구체적으로 다음과 같습니다.

- 변화하는 데이터 개인정보 보호 환경에 대한 Cloudflare의 견해
- 데이터 개인정보 보호 및 데이터 요청에 대한 Cloudflare의 정책

변화하는 데이터 개인정보 보호 환경

클라우드 서비스가 폭발적인 증가하고 데이터를 만든 사람이 거주하지 않는 국가에 데이터가 보관될 수 있다는 사실은 법 집행 조사를 수행하는 정부에 대한 도전이 되었습니다. 모든 종류의 온라인 서비스 공급자들은 그러한 전자 기록의 액세스 포인트로 기능하는 경우가 많습니다.

Cloudflare와 같은 서비스 공급자의 경우, 데이터에 대한 정부 요청은 난처한 상황을 가져올 수 있습니다. 법 집행 기관 및 기타 정부 당국이 하는 일은 중요합니다. 동시에 법 집행 기관 및 기타 정부 당국이 Cloudflare에서 찾는 데이터는 Cloudflare의 것이 아닙니다. Cloudflare의 고객은 Cloudflare의 서비스를 이용함으로써 해당 데이터에 대해 Cloudflare를 신뢰하는 것입니다. 이러한 신뢰를 유지하는 것은 Cloudflare 사업과 Cloudflare 가치의 근본입니다.

정부마다 개인 데이터 보호에 대해 상이한 기준을 갖고 있으므로 이러한 긴장 상태는 더욱 복잡해집니다. 예를 들어, 미국은 법적으로 규정된 특정한 경우를 제외하면 외국 정부를 대상으로 하는 경우를 포함, 통신 내용 공개를 금지합니다. 오랫동안 개인정보 보호를 기본적인 인권으로 간주해 온 유럽 연합(EU)에서는 개인정보 보호 일반 규정(General Data Protection Regulation, GDPR)을 통해 EU 거주자의 개인 데이터를 보호합니다. 이러한 보호 방식은 중복되는 측면도 있지만, 범위와 보호 대상에서 모두 차이가 있습니다.

이러한 법적 틀 간의 차이점은 중요하며, 특히 외국 정부의 정보에 대한 법적 요청이 개인정보 보호 요구 사항과 일치하는지를 판단할 때 더욱 중요합니다. 예를 들어, 최근 유럽 연합 사법 재판소(CJEU)는 여러 차례에 걸쳐 개인 정보 실드(또는 이전의 미국-EU 간 세이프 하버) 등의 자발적 약속과 함께 데이터 수집에 대한 미국의 법적 제약이 EU 정보 보호 요건과 부합하지 않는다고 결론 내린 바 있습니다. 주된 이유는 미국 법에 따라 사법 당국이 첩보의 목적으로 미국 시민이 아닌 자에 대한 정보를 수집할 수 있기 때문입니다. 실제로, 유럽 데이터 보호위원회(EDPB)는 생성되는 데이터에 대해 EU가 통제력을 유지할 수 있는 법적 절차를 벗어난 데이터에 대한 미국 형법 상의 요청이 GDPR의 대상인 개인 데이터를 전송할 수 있는 합법적인 근거가 되지 않는다는 입장을 유지해 왔습니다.

이는 근본적으로 한 나라의 정부가 법적 명령 등의 법적 절차를 통해 다른 국가 국민의 데이터에 접속할 수 있는 것이 적절한 경우가 어떤 경우인지에 대한 분쟁입니다. 또한, 이러한 분쟁은 유럽에서만 일어나는 것도 아닙니다. 국가마다 정책적인 대응은 다르지만, 자국 국민의 데이터에 대한 액세스를 국가 보안 문제로 보는 국가가 늘어나고 있습니다.

데이터 개인정보 보호와 데이터 요청에 대한 Cloudflare의 정책

Cloudflare에서는 개인 데이터 액세스에 대한 우려를 다루는 정책을 오랫동안 유지해 왔습니다. 이는 그렇게 하는 것이 옳다고 믿기 때문이며, 오늘날 목도하는 법적 충돌이 불가피하다고 생각했기 때문이기도 합니다. 이러한 정책에는 다음이 포함됩니다.

- 개인 데이터를 처리하는 방법 및 해당 데이터에 대한 법 집행 요청에 대응하는 방법에 대한 공개적 약속
- 데이터 요청에 대해 고객에게 알리는 방법.

일반적으로 두 가지 법적 표준 사이에 충돌이 있는 경우 Cloudflare에서는 개인정보를 가장 잘 보호할 수 있는 표준을 기본으로 합니다. 또한, Cloudflare에서는 항상 법적 절차를 요구합니다. 데이터로 향하는 문을 일단 열게 되면 닫기가 쉽지 않기 때문입니다.

개인 데이터 및 법 집행 요청에 대한 Cloudflare의 공개적 약속

Cloudflare에서는 데이터 관련 법 집행 요청에 대한 상세 정부 보고를 포함한 2013년 첫 번째 투명성 보고서를 시작으로 데이터에 대한 요청에 어떻게 대응할지에 대해 공개적으로 약속하고 Cloudflare에서 하지 않은 일에 대한 공개 약속을 해왔습니다. Cloudflare에서 하지 않은 일에 대한 공개 진술을 영장 '카나리아'라고 부르는데, 이는 외부 세계에 중요한 메시지를 전달하는 역할을 한다고 생각합니다.

'카나리아'는 두 가지 기능을 합니다. 첫째, Cloudflare가 이러한 행동을 자발적으로 취하지 않을 것이라는 공개적 진술입니다. 둘째, 이러한 진술을 사이트에서 삭제한다면 Cloudflare가 다른 방식으로 공개하는 것이 제한될 수 있다는 정보를 전달하는 기제가 될 수 있습니다.

규제 당국은 개인정보 보호 약속(특히, 이러한 약속이 계약에 의해 강제화될 경우)의 가치를 인식하기 시작했습니다. 실제로, Cloudflare가 수년 동안 투명성 보고서에 포함한 공개 약속은 유럽 연합 위원회가 GDPR을 준수하기 위한 표준 문안 초안에 포함하도록 권장하고 있는 약속과 정확히 일치합니다.

본 백서 발간일 현재 Cloudflare에서 약속하는 사항의 몇 가지 예는 다음과 같습니다.

- **Cloudflare에서는 Cloudflare 네트워크에 법 집행 소프트웨어나 장비를 설치한 적이 없으며, Cloudflare 네트워크를 통과하는 컨텐츠를 제공한 적이 없습니다**. Cloudflare는 보안 회사로서, Cloudflare 네트워크에 대한 액세스를 통제하는 것이 절대 명제임을 잘 알고 있습니다. 그래서 Cloudflare 보안팀에서는 접근 제어, 로깅, 모니터링에 초점을 맞추고 매년 수 차례 제삼자의 평가를 받습니다. 이러한 통제에는 법 집행 기관이나 정부 당국에 대해 예외가 없다는 것을 고객에게 확실히 알리고자 합니다. 그렇기 때문에 Cloudflare에서는 Cloudflare 네트워크 어디에도 법 집행 소프트웨어나 장비를 설치한 적이 없으며 Cloudflare 네트워크를 통과하는 고객의 컨텐츠를 정부 기관에 제공하지 않았다고 진술하고 있습니다.
- **Cloudflare는 인증 키의 암호화 방식을 공유한 적이 없습니다.** Cloudflare는 온라인상에서 개인정보 보호를 위해 컨텐츠 및 메타데이터 모두를 강력하게 암호화해야 한다고 믿습니다. 한 나라가 자국민의 개인정보에 대한 다른 나라 정부의 접근을 막으려 한다면 해당 개인정보의 암호화가 우선되어야 합니다. 하지만 고객과 규제 기관 또한 암호화 자체가 신뢰할 수 있다고 확신해야 합니다. 따라서 Cloudflare는 Cloudflare의 암호화 방식 및 인증 키(또는 고객의 암호화 방식 및 인증 키)를 누구에게도 넘기지 않았으며 법 집행 기관이나 기타 제삼자의 요청에 따라 암호화를 약화하거나 손상하거나 와해하지 않았다고 약속합니다.
- **Cloudflare는 고객 컨텐츠 또는 DNS 요청을 수정한 적이 없습니다.** Cloudflare는 시스템을 악용해 방문하고자 하는 사이트가 아닌 사이트로 안내하거나 온라인에서 얻는 컨텐츠를 변경해서는 안 된다고 믿습니다. 따라서 Cloudflare는 법 집행 기관이나 기타 제삼자의 요청에 따라 고객 컨텐츠를 수정하거나 DNS 응답의 대상을 수정한 적이 없다고 공개적으로 진술했습니다.
- **잠재적인 약속 위반에 대한 투명성**: Cloudflare에서는 필요 시 이러한 약속을 위반하도록 강요하는 법적 명령에 대해 이의를 제기하겠다고 약속했습니다. 저희는 Cloudflare의 고객 뿐 아니라 전 세계 각국의 정부에 대해서도 Cloudflare가 선을 긋고 있는 지점에 대해서도 목표가 명확합니다.

데이터 보호에 대한 Cloudflare의 전반적인 철학은 창사 이래 변함이 없었지만, Cloudflare에서 Cloudflare의 최신 제품과 정책 환경의 변화를 반영하기 위해 이러한 약속을 조정하는 일도 있습니다. 이러한 약속의 최신 목록은 투명성 보고서 페이지에서 확인할 수 있습니다.

고객에게 정부 요청 통지 제공

Cloudflare에서는 법 집행 기관이나 기타 정부 기관을 포함하는 누구라도 법적 절차를 이용해 고객의 데이터를 요청하는 경우, 고객이 이에 대해 통지를 받아야 한다고 오랫동안 믿어 왔습니다. 고객은 이러한 통지를 통해 문제가 있는 경우 해당 요청에 이의를 제기할 수 있습니다.

실제로, Cloudflare에는 회사 설립 초기부터 고객에게 통지하는 정책이 있습니다. Cloudflare 직원이 30명이 채 안 되던 2013년, FBI에서 국가 안보 서신을 들고 회사에 와서 한 고객에 대한 정보를 요청하고 Cloudflare의 변호사가 아닌 누구와도 이에 대해 논의하지 못하도록 한 적이 있습니다. 당시의 국가 안보 서신은 아무런 제재 없이 미국 정부의 아무 부서에서든 작성하고 집행할 수 있었으며 수신자는 이에 대해 영원히 말할 수 없었습니다.

Cloudflare는 조사의 실행 가능성을 보존하기 위해 공개를 일시적으로 제한하는 것이 법 집행에 적합한 경우도 있을 수 있다는 점을 인정합니다. 하지만 정부는 어떠한 비공개 조항도 정당화하여야 하고 어떠한 비공개 조항도 현재의 목적에 필요한 최소한의 시간으로 제한되어야 한다고 생각합니다. 그래서 Cloudflare는 전자 프론티어 재단(Electronic Frontier Foundation)과 협력하여 그 서신에 대해 이의를 제기했습니다. 그 결과 법원 소송은 몇 년 동안 지속되었고 2017년까지 이에 대해 이야기할 자격이 없었습니다. 하지만 FBI는 궁극적으로 서신을 취하했습니다.

미국 법원이 무기한 비공개 명령은 헌법상의 문제를 야기한다고 시사했으므로 미국 법무부에서는 2017년, 예외적인 경우를 제외하고는 연방 검찰에게 비공개 명령을 1년 이하로 제한하도록 지침을 내렸습니다. 그러나 이는 미국의 모든 법 집행 기관에 대해 무기한 비공개 명령을 중지한 것은 아닙니다. 2017년 이후 본 백서 발간일까지 Cloudflare는 종료 일자가 포함되지 않은 비공개 명령을 28건 이상 받았습니다. Cloudflare에서는 이러한 비공개 명령을 받으면, 미국 시민 자유 연맹(ACLU)과 협력하여, 소송을 제기하겠다고 하였습니다. 모든 경우에서 정부 기관은 해당 명령의 비공개 명령에 시간 제한을 삽입하였고 Cloudflare는 고객에게 이러한 요청에 대해 통지할 수 있었습니다.

법적 충돌 해결

GDPR과 같은 법규를 준수하려면, 특히 당사가 이러한 법규를 위반해야 하는 어려운 상황에 처하게 되는 법적 명령에 직면한 경우, 이러한 법규를 준수하려면 법원이 필요합니다. Cloudflare와 같은 서비스 공급자는 법적 충돌을 이유로 법원이 법적 요청을 각하하도록 요청할 수 있고 Cloudflare에서는 공개 진술과 계약상의 데이터 처리 부록(DPA)에서 이러한 법적 충돌을 피하기 위해 필요한 경우, 해당 절차를 밟겠다고 약속해 왔습니다. 법적 충돌은 충돌의 출발점 즉 정보에 대한 접근 권한을 얻을 수 있는 자격에 대해 분쟁하는 두 국가 간의 문제로 귀결되어야 한다는 것이 Cloudflare의 견해입니다.

결론

본 백서는 데이터 개인정보 보호에 대한 Cloudflare의 광범위하고 심층적인 약속을 소개하는 것에 불과합니다.

자세한 내용은 다음을 참조하시기 바랍니다.

- **Cloudflare의 개인정보 취급 방침**: Cloudflare에서 수집하는 데이터, 사용 방법, 공유하는 데이터, 기타 일반적인 개인정보 보호 관련 문제를 다룹니다.
- **Cloudflare의 투명성 보고서**: 고객에 대한 정보를 공개하도록 요구한 법적 요청에 대한 최신 정보.
- **Cloudflare의 데이터 개인정보 보호 및 규제 준수 홈 페이지**: Cloudflare의 정책 및 제품이 개인정보 보호 및 규제 준수 요건을 어떻게 충족하는지에 대한 최신 공식적 발표.

궁극적으로, 고객과 최종 사용자의 데이터를 보호하고 전세계의 다양한 개인정보 보호법을 준수하는 전역 네트워크를 운영하려면, 원칙을 지키고 투명하며 개인정보를 존중하고 합당한 절차를 요구하며 고객 스스로 데이터에 대해 결정할 수 있도록 고객에게 통지한다는 Cloudflare가 처음부터 지탱해 온 가치로 돌아가야 합니다.

CLOUDFLARE

007-9814-2030-192 | enterprise@cloudflare.com | cloudflare.com/ko-kr

REV:BDES-5987.2024JUL29