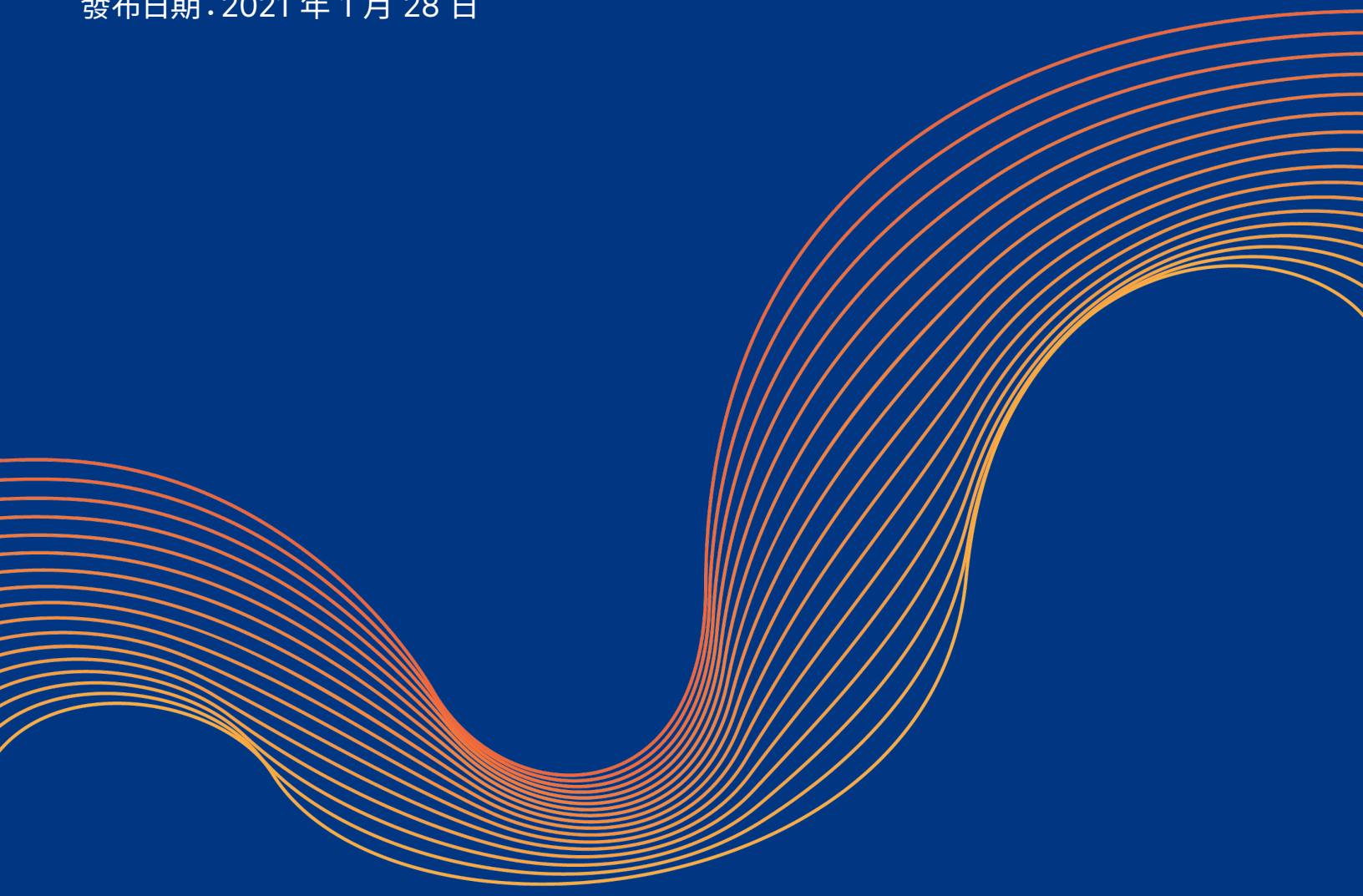
白皮書

CLOUDFLARE

Cloudflare 關於資料隱私權和執法機關要求的原則

發布日期：2021 年 1 月 28 日



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

Cloudflare 的網路和業務最終都建立於客戶信任的基礎之上。透過組建和部署有助於提高我們系統安全性的產品，加密靜態資料或傳輸中資料，並允許我們的客戶決定世界各地的流量如何接受檢查，我們尋求不斷贏得和維護這種信任。

但並非所有挑戰都能透過工程技術來解決。因此，我們也有原則和程序來指導我們如何管理系統上的客戶和最終使用者資料，以及如何處理政府和其他與資料有關的法律要求。

本文概述這些原則，並就我們在資料隱私權和合規方式等各方面的詳細資訊提供了連結。具體包括如下內容：

- 我們有關不斷變化的資料隱私權形勢的觀點
- 我們有關資料隱私權和資料要求的原則

不斷變化的資料隱私權形勢

雲端服務的爆炸式增長，以及資料可能儲存於資料產生者所在國以外這個事實，給各國政府的執法調查構成了挑戰。各種各樣的線上服務提供者常常充當這些電子記錄的存取點。

對於 Cloudflare 這樣的服務提供者，政府對資料的要求可能令人擔憂。執法機構和其他政府部門開展的工作至關重要。而與此同時，執法機構和其他政府部門向我們索取的資料卻又不屬於我們。客戶使用我們的服務，意味著他們信任我們可以保護其資料。維護這種信任是我們業務和價值觀的基石。

不同政府在個人資料的保護方面訂立了不同的標準，進一步加劇了這種緊張局面。例如，美國禁止公司公開通訊的內容，包括向非美國政府，僅某些法律規定的情形例外。歐盟長期以來認為隱私權是一項基本人權，透過《一般資料保護規定》(GDPR) 保護所有歐盟個人資料。儘管這些保護在某些方面有所重疊，但在範圍和保護對象上各有不同。

法律框架之間的差異很重要，尤其是在來自外國政府的資料要求是否符合隱私權要求時。例如，近年來，歐盟法院 (CJEU) 在多個場合得出結論：美國對收集資料的法律限制，以及某些自願承諾 (如隱私權護盾，或其前身 [美國-歐盟安全港]) 不足以符合歐盟隱私權規定，這主要是因為美國法律允許執法機構為外國情報目的而收集非美國公民的資訊。事實上，歐洲資料保護委員會 (EDPB) 採取的立場是，美國刑法在法律程序以外提出的資料要求 (而在該等法律程序中，歐盟國家對所產生的資訊擁有一定控制權)，並不構成 GDPR 個人資料主體轉移的合法依據。

本質上，這些爭論的焦點在於：某國政府究竟何時使用法律命令或其他法律程序來獲取另一國家公民資料才是恰當的。儘管各國對這些原則的回應並不一致，但越來越多的國家現在已將獲取其公民資料視為國家安全問題。

Cloudflare 有關資料隱私權和資料要求的原則

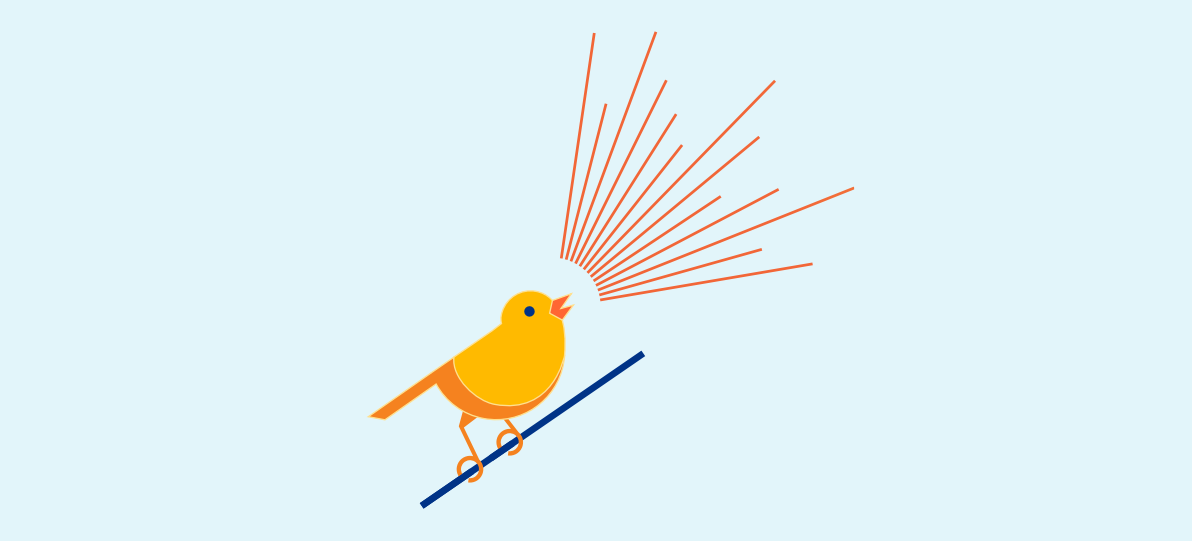
Cloudflare 長久以來建立了各種原則來處理與獲取個人資料相關的問題。
我們之所以這樣做，一方面是我們認為這是正確的做法，另一方面是我們今天所看到的法律衝突似乎是不可避免的。這些原則包括：

- 有關我們如何處理隱私資料以及如何處理執法機關對該等資料的要求的公開承諾
- 我們如何將對資料的要求知會客戶。

一般而言，當兩種不同的法律標準存在衝突時，我們預設選擇最能保護隱私權的標準。而且我們始終要求遵守法律程序。這是因為獲取資料的大門一旦打開，就再也難以關上。

我們有關隱私資料和執法機關要求的公開承諾

從我們 2013 年詳細闡述執法機關要求的首份透明度報告開始，我們已經就我們處理資料要求的方式做出了公開承諾，並就我們從未做過的事發表了公開聲明。我們將有關從未做過的事的公開聲明稱為 [金絲雀] 安全聲明，目的是起到向外界發出信號的作用。



這些 [金絲雀] 有兩個作用。首先，公開表明我們並非自願採取這些行動。其次，透過從網站上刪除該聲明，這可以成為一種傳遞資訊的機制，暗示我們可能被限制公開這些資訊。

監管機關已經開始認識到隱私權承諾的價值，尤其在承諾可透過合約強制執行時。事實上，多年來包含在我們透明度報告中的承諾，與歐盟委員會建議在為了遵守 GDPR 而起草的《標準合約條款》中所包含的承諾類型完全一致。

截至本文發布之日，我們所做承諾的主要範例如下：

- **我們從未在我們的網路上安裝過執法軟體或設備，或供給我們網路上所傳輸的內容：**作為一家安全公司，我們知道，始終控制對我們網路的存取是絕對必要。因此，我們的安全團隊一直專注於存取控制、記錄和監視，並每年進行多次第三方評估。我們要確保客戶能瞭解，在這些控制中，不存在對執法機關或政府行為者的任何豁免。
  因此，我們承諾，Cloudflare 從未在我們網路的任何位置安裝過執法軟體或設備，我們也從未向任何政府機構供給我們網路上所傳輸的內容。
- **我們從未共用過加密或認證金鑰：**Cloudflare 認為，強加密 (包括內容加密和中繼資料加密) 對於線上隱私權非常必要。如果一個國家希望防止另一個政府獲取其公民的個人資訊，第一步應當是加密該等個人資訊。而客戶和監管機構也需要確信，加密本身是值得信賴的。因此，我們承諾，我們永遠不會將我們 (或我們客戶的) 加密或認證金鑰移交給任何人，我們永遠不會應執法部門或任何其他第三方的要求而削弱、降級或破壞我們的加密。
- **我們從未修改過客戶內容或 DNS 請求：**我們認為，我們的系統不應被利用來將人們引導到他們不打算瀏覽的網站，或修改他們線上獲得的內容。因此，我們已公開聲明，我們從未應執法機構或任何第三方的要求而修改客戶內容或修改 DNS 回應的預期目的地。
- **對可能違背承諾的情形保持透明度：**我們已承諾對任何要求我們違背這些承諾的法令提出質疑，必要時訴諸法庭。我們的目標是，無論是對我們的客戶還是世界各國政府，我們的界線都非常明確。

雖然我們有關資料保護的整體理念自創立以來從未改變，但我們偶爾也會調整承諾，以反映產品和原則環境的最新變化。這些承諾的最終和最新清單請參見透明度報告頁面。

將政府要求知會客戶

Cloudflare 一直認為，在任何人 (包括執法機構或其他政府行為者) 使用法律程序來要求客戶資料時，客戶應當得到通知。在得到通知後，如果客戶存在顧慮，就可以質疑該等要求。

事實上，自本公司創立之初，我們的原則便是及時將有關事宜告知客戶。2013 年 1 月，我們只有不到 30 名員工時，聯邦調查局 (FBI) 帶著一封國家安全函出現在我們門前，要求提供一位客戶的資訊，並禁止我們與律師以外的任何人討論此事。當時，國家安全函幾乎不受任何監管，可由美國政府的單一部門簽發和執行，並無限期禁止收件方討論它們。

我們承認，在某些情況下，為了不妨礙案件調查，執法部門可能需要暫時限制資訊公開。然而，我們也認為，應當要求政府部門證明任何保密條款的合理性，且任何保密條款都應當具有明確的時效性，不能超過達到相應目的所需的最短時間。因此，我們與電子前線基金會 (Electronic Frontier Foundation) 合作，對該信函發起了法律質疑。

由此產生的訴訟持續了幾年，而且在 2017 年以前我們一直被禁止談及此事。但最終，FBI 撤回了該信函。

由於美國法院提出的無限期保密命令引發憲法問題，美國司法部於 2017 年發布指引，要求聯邦檢察人員將保密命令的時間限制為不超過一年，除非有特殊情況。然而，仍有美國執法機構簽發無限期保密命令。截至本文發布之日，我們自 2017 年以來已收到 28 份沒有結束日期的保密命令。每當收到此類無限期保密命令時，Cloudflare 都會與美國公民自由聯盟 (ACLU) 合作，提出訴訟警告。每一次，政府隨後都會在這些命令的保密要求中加上時間限制，允許我們將有關要求知會客戶。

解決法律衝突

若要始終遵守 GDPR 等法律，尤其是當所收到的法律命令可能導致我們處於被迫違反此等法律的艱難境地時，需要我們訴諸法院。像 Cloudflare 這樣的服務提供者可能會因法律衝突而要求法院撤銷這些法律要求，而且我們已經同時透過公開聲明和合約做出了以下承諾：我們會在必要時採取上述措施來避免此等衝突。我們的觀點是，這種衝突應當從源頭解決，即由爭奪資訊獲取權的兩個政府來解決這種衝突。

結論

本文僅僅初步介紹了我們在資料隱私權方面廣泛而深入的承諾。
如需進一步瞭解這些承諾，請查閱：

- 我們的整體隱私權政策：涵蓋我們所收集的資料、使用資料的方式、所共用的資料，以及其他常見的隱私權問題。
- 我們的透明度報告：及時通報我們所收到的公開客戶資訊的法律要求。
- 我們的資料隱私權與合規首頁：有關我們的原則和產品如何支援隱私權和合規需求的最新公告。

最後，為了建立一個全球網路來保護客戶和最終使用者資料並遵守世界各地的不同隱私權法律，必須回歸到我們公司創立以來所倡導的價值觀：堅持原則和透明，尊重隱私權，要求合理程序，並知會客戶以便後者就其資料自行做出決定。