Everbridge Notice on U.S. Government Requests and U.S. Signals Intelligence Safeguards in the context of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "DPF")

LAST UPDATED: January 8, 2026.

Introduction

This notice focuses on (i) U.S. government access risks relevant to EU/UK/Swiss transfers addressed in Schrems II and (ii) safeguards and redress mechanisms underpinning the Data Privacy Frameworks (the EU-U.S. Data Privacy Framework, and, as applicable, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, collectively hereinafter, "DPF"). It does not describe every type of U.S. legal process.

On July 16, 2020, in the *Schrems II* decision, the Court of Justice of the European Union invalidated the EU-US Privacy Shield framework, but upheld the validity of the European Commission's standard contractual clauses ("SCCs") as a cross-border transfer mechanism for personal data leaving the European Economic Area ("EEA"). While the SCCs remain valid, organizations that currently rely on them must consider whether, with regard to the nature of the personal data they possess, the purpose and context of the processing, and the country of destination, there is an "adequate level of protection" for the personal data as required EU law, and where there is not, consider what additional safeguards may be implemented to ensure there is an adequate level of protection.

On October 7, 2022, in response to concerns raised in *Schrems II*, the United States issued Executive Order 14086 (Enhancing Safeguards for United States Signals Intelligence Activities), which introduced additional safeguards for U.S. signals intelligence activities and established a redress mechanism that includes independent review by the Data Protection Review Court (DPRC). On July 10, 2023, the European Commission adopted its adequacy decision for the DPF, which enables eligible transfers to participating U.S. organizations.

In September 2025, the EU General Court dismissed an action seeking annulment of that adequacy decision in *Latombe v Commission*.

Everbridge Inc. ("Everbridge" or "we") monitors for material legal developments affecting the DPF and updates this notice as appropriate.

Everbridge Transfers

Everbridge no longer relies on the EU-U.S. Privacy Shield framework to support transfers of data. It participates in and relies upon the DPF for eligible, in-scope transfers.

Where the DPF is not available or is not relied upon for a particular transfer, Everbridge relies on the European Commission's Standard Contractual Clauses (SCCs), supported by transfer impact assessments and supplementary measures, as appropriate. These measures are specifically included in our standard Data Processing Agreement (DPA) with our business interlocutors, including vendors and sub-processors. Everbridge incorporates the EU's revised SCCs, issued on June 4, 2021, into its DPAs. For more information on our compliance with EU transfer requirements, please see our white paper available at:

https://www.everbridge.com/about/legal/everbridge-transfer-requirements-paper

Everbridge has certified to the U.S. Department of Commerce that, where possible, we adhere to the DPF Principles with regard to the processing of personal data we receive from the European Union, the United Kingdom, and Switzerland when we rely on the DPF as the relevant transfer mechanism for that data. For transparency, Everbridge may use other transfer mechanisms (such as SCCs) where appropriate and as reflected in applicable customer agreements (e.g., the DPA).

To learn more about the DPF Principles, and to view our registration, please visit https://www.dataprivacyframework.gov/. Refer to the Everbridge Global Privacy Notice at https://www.everbridge.com/about/legal/everbridge-global-privacy-notice/.

Customer Personal Data Processing Generally

- **Security Controls:** Everbridge has a robust information security program that is aligned with industry recognized standards such as ISO 27001-or SOC 2, where applicable. Everbridge's information security management system was inspected and certified by an accredited certifying body and the certificate is available at https://www.trust.everbridge.com.

- **Sub-processors**: Everbridge's sub-processors are contractually committed to adhere to appropriate data privacy and information security controls. For a complete list of Everbridge sub-processors, please go to https://www.everbridge.com/about/legal/everbridge-sub-processors.

- **Amazon Web Services (AWS)** is one of Everbridge's primary sub-processors. AWS has published their own response to the Schrems II decision, which includes their commitment to challenge law enforcement requests, which is available at:

  https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data

- **Customer service/support:** Everbridge relies on several sub-processors to ticket, build knowledge base articles and manage service/support requests related to our products. These servers are located in the US. The personal data processed in these systems is limited to general contact information (e.g., name, email, phone).***Customers should never enter any personal data in the body of service/support tickets beyond that of the requester, including sensitive or special category data.***

- **Analytics:** Everbridge utilizes sub-processors to collect web analytics to improve its products and services, and for logging analytics. These servers are located in the US. The personal data processed is limited to general contact information, usually email for web analytics, and user access metadata for logging analytics.

- **Message delivery:** sub-processors facilitate the delivery of messages to Everbridge mobile applications, and may process name, phone number, device identifier, and location data. Sub-processors may use servers located in the US. Everbridge provides only the minimum amount of data to sub-processors necessary to furnish the services, which is generally only phone numbers for the purpose of sending text messages.

- **Communications Delivery Channels:** Everbridge also receives support in delivery of communications to systems and devices, such as phones, pagers, apps, and TTY/TTD. These services may receive personal data including addressing (e.g., email, phone number) and user-provided message content. Some services use servers located in the US for processing. Everbridge provides only the minimum amount of necessary data to provide the

services, which is generally an address component and the user-provided message content for the purpose of delivering the communication.

- **Minimum necessary:** We apply a "minimum necessary" approach to PII handling consistent with our customers' policies and applicable requirements.
- **Breach notification to customers:** If Everbridge discovers a breach of unsecured data, we will notify the affected customer(s) without unreasonable delay as required by multiple regulations and customers' service agreements.

Government Requests for Customer Data

As noted in the introduction, the court in *Schrems II* was principally concerned with the ability of US law enforcement to reach EU personal data through mechanisms such as Foreign Intelligence Surveillance Act (FISA) Section 702 and other intelligence gathering activities under Executive Order (E.O) 12.333, plus certain compelled disclosure by authorities under U.S. law (including the Electronic Communications Privacy Act and related statutes). The US Department of Commerce published its formal response to the decision in September 2020 specifically to address questions and concerns about the use of these mechanisms to reach personal data, which we encourage customers to review.

Compelled disclosure may include non-notification or delayed-notice requirements in some circumstances. U.S. law may also, in certain circumstances, compel production of data within a provider's possession, custody, or control regardless of where the data is stored (e.g., under the Stored Communications Act and amendments commonly referred to as the "CLOUD Act"), subject to applicable legal standards and available challenges in cases of qualifying conflicts of law.

We note that under Section 3 of the October 7, 2022 Executive Order, should an individual from a qualifying state (including the European Union) believe the individual has been harmed by U.S. signals intelligence activities, the individual may submit a complaint through the relevant redress mechanism regarding U.S. signals intelligence activities, consistent with Executive Order 14086 and implementing procedures.

Although Everbridge could in some circumstances be considered an electronic communications service provider under a broad reading of these authorities, as of the effective date of this notice, Everbridge has never received a request for customer personal data under FISA 702, E.O. 12.333, or the ECPA.

If Everbridge does receive a court or other order for customer personal data under FISA 702, EO 12,333, or the ECPA, Everbridge will:

- Notify the affected customer of any request that Everbridge provide its data, or access to its data, by a law enforcement or other government agency unless we are explicitly prohibited from doing so, or unless we reasonably determine notification is not permitted, and afford the customer the opportunity to challenge the order prior to compliance if it is possible to do so.
- Whenever possible, we will refer the government agency to the affected customer to fulfill the request rather than providing the data directly.
- We will challenge unlawful requests and only disclose customer data to government agencies when compelled by law.
- If we are required to disclose customer data to government agencies, we will provide only the data strictly required by the order based on a reasonable interpretation.

- We apply internal review and escalation procedures designed to ensure government requests are evaluated for legal validity, scope, and minimization.
- Where legally permissible, we will seek to narrow requests and associated non-disclosure obligations and will use reasonable efforts to lift prohibitions on customer notice.

HIPAA/ePHI Information

Some Everbridge products and services may be used by healthcare customers and other entities that are subject to the U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Where Everbridge acts as a "business associate" and processes protected health information ("PHI") on behalf of a customer, Everbridge's HIPAA obligations are addressed in the parties' Business Associate Agreement ("BAA") and applicable HIPAA requirements. Additionally:

- **Safeguards for ePHI:** Everbridge maintains specific administrative and technical safeguards designed to protect electronic PHI, consistent with applicable HIPAA Security Rule requirements (e.g., access controls and audit controls).
- **Sub-processors:** where Everbridge uses sub-processors to create, receive, maintain, or transmit PHI on Everbridge's behalf, Everbridge requires appropriate written commitments and restrictions consistent with HIPAA business associate requirements.

See further disclosures at: https://www.everbridge.com/about/legal/everbridge-privacy-practices-for-medical.

Contact Information

For questions about this position statement, please contact privacy@everbridge.com. For more information about Everbridge Corporation's data privacy program, please visit our company website.