Everbridge Notice on the EU-U.S. Data Privacy Framework (DPF), UK Extension to the EU-U.S. DPF, Swiss-U.S DPF, and U.S. Enforcement Requests

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 *Schrems II,* the United States Government issued a new Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, and in large part rescinded Presidential Directive 28, which had authorized certain intelligence gathering activities that the *Schrems II* decision found rendered the Privacy Shield framework inadequate. The new framework, referred to as "Privacy Shield 2.0," provides a specific redress procedure for individuals who believe they have been harmed by the U.S. government's intelligence activities, including the establishment of the Data Protection Review Court.

Everbridge no longer relies on the EU-US Privacy Shield framework, nor does it intend to rely on "Privacy Shield 2.0." to support transfers of data. Rather, Everbridge relies on the SCCs for transfer of personal data and these are specifically included in our standard Data Processing Agreement (DPA) with our business interlocutors, including vendors and subprocessors. Everbridge is incorporating the EU's revised SCCs, issued on June 4, 2021, into our 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.

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.

• **Subprocessors:** Everbridge's subprocessors are contractually committed to adhere to appropriate data privacy and information security controls. For a complete list of Everbridge subprocessors, please go to https://www.everbridge.com/about/legal/everbridge-sub-processors/. Amazon Web Services (AWS) is one of Everbridge's primary subprocessors. 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 ZenDesk, Ariglad and AptEdge to ticket, build knowledge base articles and manage service/support requests related to our products. These servers 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 sensitive or special category data in the body of service/support tickets. Indeed, no personal data beyond that of the requester should be included.

• **Analytics:** Everbridge uses Pendo and Totango to collect web analytics to improve its products and services, and Sumo Logic and Splunk 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:** PubNub facilitates the delivery of messages to Everbridge mobile applications, and may process name, phone number, device identifier, and location data. PubNub uses servers located in the US. Everbridge provides only the minimum amount of data to PubNub needed to provide the services, which is generally just phone numbers for the purpose of sending text messages.

• **Communication 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, and some services use servers located in the US for processing. Everbridge provides only the minimum amount of data to needed to provide the services, which is generally an address component and the user provided message content for the purpose of delivering the communication.

Government Requests for Customer Data

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, as well as "no knock" warrants under the Electronic Communications Privacy Act (ECPA), which allow for records requests to electronic communications service providers and generally do not permit immediate notification to the data subject of the existence of the order. The US Department of Commerce published its formal response to the decision in September 2020 to specifically address questions and concerns about the use of these mechanisms to reach personal data, which we encourage customers to review.

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 they have been harmed by U.S. signals intelligence activities, they may seek redress directly with the U.S. Government.

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

In the event that 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, 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.

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.