Everbridge Notice on Compliance with EU, UK, and Swiss Transfer Requirements for Personal Data

Everbridge is committed to supporting its customers in their privacy compliance. Everbridge was a participant in Privacy Shield before it was invalidated in the EU, and where possible, continues to participate in the new EU-US Data Privacy Framework, as well as the UK Extension to the DPF and the Swiss-US Data Privacy Framework (collectively, the "DPFs"). Nonetheless, we understand that transfers of personal data from the EU to the US can be complex, and this notice is designed to provide Everbridge customers and end users with information about Everbridge's compliance with the recommendations of the European Data Protection Board to help ensure adequate protections of personal data transferred to the United States.

This document is for reference purposes only and does not modify any terms of any agreement with Everbridge, and Everbridge assumes no liability arising from your use of the information in this notice.

Introduction

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a new Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, and in large part rescinded Presidential Directive 28, which had authorized certain intelligence gathering activities that the *Schrems II* decision found rendered the Privacy Shield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 DPF 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.

European Data Protection Board Recommendations

After the *Schrems II* ruling, the European Data Protection Board ("EDPB") published recommendations on supplemental measures companies should implement to ensure adequate protection of personal data transferred outside the EU. While these recommendations are non-binding, Everbridge has used them to assess transfers of personal data. The recommendations include six steps:

1. **Know Your Transfers**: Record and map all transfers and assess whether the personal data transferred is limited to only what is necessary.

Everbridge may transfer personal data out of the EEA and UK for processing depending on the product or service you are using. For specific information regarding the types of personal data collected by Everbridge products, as well as any international transfers of that data, please review the Global Privacy Notice, available here: https://www.everbridge.com/about/legal/everbridge-global-privacy-notice.

Everbridge's subprocessor list is published here: https://www.everbridge.com/about/legal/everbridge-sub-processors/.

The list identifies each subprocessor, its location, and the purpose of processing, and includes a link to that subprocessor's privacy policies. We update this list on an ongoing basis as needed.

2. **Identify Your Tools**: In the absence of an adequacy decision, a transfer tool containing appropriate safeguards under Article 46 of the GDPR should be used (SCCs, binding corporate rules, codes of conduct, certification mechanisms, and ad hoc contractual clauses).

Everbridge relies on both the DPF and the current SCCs and UK Addendum to the SCCs for transfer of personal data. In addition, Everbridge has adopted an intracompany data transfer agreement that contains the SCCs with the UK Addendum.

3. **Asses the Transfer Tool in Light of All Circumstances:** Consider whether there is anything in the law or practices of the third country that may impinge on the effectiveness of the safeguards.

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, or "no knock" warrants under the Electronic Communications Privacy Act (ECPA), authorized by a court, 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. We encourage customers to read this white paper.

Please also review our Notice on U.S. Enforcement requests here: https://www.everbridge.com/about/legal/everbridge-law-enforcement-requests-paper.

To date, Everbridge has never received such a request for customer personal data under FISA 702 or E.O. 12.333 or the ECPA.

4. **Adopt Supplementary Measures**: If the previous step shows that the transfer tool is not effective in protecting personal data, in collaboration with the exporter, determine what supplementary measures could be adopted to ensure the data receives an adequate level of protection.

This step is only required if the assessment of the effectiveness of the transfer mechanism indicates supplementary measures are needed, and we do not believe additional steps are required beyond the DPF and SCCs and our other safeguards. Everbridge requires its vendors and subprocessors to meet appropriate data security standards and data privacy requirements. Everbridge has a robust information security program that is aligned with industry recognized standards such as ISO 27001 or SOC 2, where applicable. A list of our standard security controls as well as our organizational, regional and functional security certifications can be found here https://www.everbridge.com/about/legal/compliance/. For security purposes, limited personnel in the United States may have access to Everbridge's systems, including systems that house customer personal data. Access to those systems is restricted and subject to the security controls detailed above.

Everbridge's sub-processors are contractually committed to adhere to appropriate data privacy and information security controls. *Note: One of Everbridge's principal sub-processors is AWS. AWS has published their own response to the Schrems II decision which includes their commitment to challenge law enforcement requests. We encourage customers to review their response.*

We also regularly update our data mapping and transfer impact assessments, and maintain a comprehensive record retention schedule and ensure data is deleted in accordance with it. We also maintain our data privacy resources on our website for reference of all our customers.

Unless required by law, Everbridge will not disclose or provide access to customer data to law enforcement. If Everbridge is compelled to disclose or provide access to customer data to law enforcement, Everbridge will promptly notify the customer and provide a copy of the demand, unless legally prohibited from doing so.

5. **Take Formal Procedural Steps**: Adopt any supplementary measures needed.

Everbridge does not believe supplementary measures are needed, therefore there are no formal procedural steps required.

6. **Reevaluate**: Monitor developments that might affect the transfers.

Everbridge stays abreast of legal developments in the US, UK, and EU, as well as other countries, to ensure that we continue to maintain protection of personal data.

Other Measures Everbridge Takes to Protect Personal Data

Data Protection Agreements

Everbridge has entered into Data Processing Agreements with affected customers and vendors which reflects GDPR requirements. Any personal data that a customer and its users upload into Everbridge systems will only be processed in accordance with the customer's or user's instructions.

Privacy by Design

Everbridge has expanded its focus on its Security by Design processes to Data Protection & Privacy by Design. Everbridge proactively applies the Data Protection & Privacy by Design principles when designing products and enhancements.

Vendor Due Diligence

Everbridge has taken steps to not only ensure its own platform GDPR compliance, but also re-evaluates its vendors through the third-party risk program for compliance.

Education and Training

Privacy training has been integrated into new hire training, annual training, and ongoing communications. These trainings ensure that the entire organization understands GDPR requirements, and are used to develop deeper, targeted trainings that cover specific obligations under the law which apply to individual groups such as marketing, customer support or engineering.

Policies and Procedures

Everbridge Privacy Notice complies with GDPR requirements and makes it easier for customers, individuals, and website visitors to understand how Everbridge handles personal data. Everbridge's global privacy program is updated and enhanced on an ongoing basis to ensure it continues to address emerging risks to data privacy and to improve protection of personal data. Everbridge also has updated and incorporated Data Protection & Privacy into its impact assessments to include a Data Protection Impact Assessment (DPIA) and better define and document the way the company performs data mapping.

Information Transferred to Everbridge in the United States

In addition to information that is transferred to subprocessors in the United States (see our subprocessor page available here: https://www.everbridge.com/about/legal/everbridge-sub-processors/), some personal data may be transferred to Everbridge in the United States for processing. Everbridge has conducted a transfer impact assessment to ensure GDPR compliance and data minimization. All such transfers occur under the auspices of an intracompany agreement that includes the SCCs with the UK Addendum, and transferred pursuant to contracts with our customers. When such a transfer includes health data, the data subject also expressly consents to the transfer.

Contact Information

For questions about this notice, please contact privacy@everbridge.com.