This white paper outlines Infobip's position and privacy practices concerning Schrems II's implications for international transfers of personal data. The information provided herein is solely for general informational purposes; it does not intend to constitute legal advice. For legal guidance, Infobip recommends that you check with a legal professional and familiarize yourself with the laws and regulations that apply to your specific situation.

Here is a quick rundown of the key points this document talks about:

- Defining the Schrems II judgment
- Impact on Infobip's products and services
- Measures implemented in Infobip
- Supporting customers in their compliance with Schrems II judgment
- How can you start using the EU Region Locked Data Center?

Defining the Schrems II judgment

At Infobip, we are committed to helping our customers comply with personal data protection laws and designing products to meet theirs and the end-user's evolving privacy needs and expectations.

We know the challenges our customers located in the EU encounter due to the personal data transfer limitations resulting from the Court of Justice of the European Union's (CJEU) Schrems II ruling (case C-311/18).

Even before the Schrems II judgment, we ensured the storage of EU customers’ information in EU-based data centers.
Following the Schrems II ruling, we took steps to support our customers by storing and processing their data in EU data centers. Additionally, we ensured that any access to personal data on our communication platform is limited to the EU and countries recognized by the European Commission as having adequate data protection measures. We also provided customer support from within the EU and these adequate countries.

What is the Schrems II judgment about?

The CJEU's decision in July 2020, known as Schrems II, determined that the United States domestic intelligence law's surveillance practices did not meet comparable EU legal standards. As a result, the CJEU invalidated the Privacy Shield agreement, which governed the transfer of personal data from the EU to the US.

However, the Schrems II ruling has implications beyond invalidating the Privacy Shield, impacting the legal landscape of all data transfers outside the EU.

Even though the CJEU's ruling confirmed the continued reliance on the European Commission's Standard Contractual Clauses (EC SCCs), it imposed additional obligations for transfers of personal data from the EU to any country that does not benefit from an EU adequacy decision.

Taking into account the impact of Schrems II judgment, the European Data Protection Board (EDPB), a body that includes representatives from data protection authorities of all EU member states, released two sets of recommendations:

- “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”,

- and “Recommendations 02/2020 on the European Essential Guarantees for surveillance measures”,

which provide guidance on measures to ensure compliance with EU-level data protection regulations. These recommendations also address the essential guarantees for surveillance measures and how companies should assess the legal framework of third countries before allowing data transfers.

In a nutshell, unless a transfer is to a country that has received the EU adequacy decision, organizations transferring and importing the data under the EC SCCs must assess the regulatory framework of the third destination country, verify that the third-country legislation is not incompatible with the EU law and, where needed, put in place additional measures to ensure an adequate level of data protection per the EU standards. The transfer can be considered unlawful if any of these preconditions are not met.

---

1An adequacy decision is a formal decision made by the EU that recognizes another country, territory, sector, or international organization that provides an equivalent level of protection for personal data as the EU does. The list of current adequacy decisions is available here. For example, following Brexit, the EC decided on the adequate protection of personal data by the United Kingdom (UK). The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein, and Iceland) to the UK without any further safeguards. In other words, transfers to the UK will assimilate into intra-EU transmissions of data.
Impact on Infobip’s products and services

The Schrems II judgment has emphasized the importance of not only having a global reach, but also providing local support. This reinforces our motto of “global reach, local presence” with added significance.

To facilitate our customers’ compliance with the Schrems II judgment when using our products and services, we, at Infobip have launched a comprehensive “EU Region-Locked Data Center Project”. The project aims to establish a secure and distinct environment within the EU.

With the EU Region-Locked Data Center project, we can now empower our customers to control personal data of their end-users and meet EU data transfer requirements imposed by the Schrems II decision.

For easier understanding, here is an overview of the deliverables we made in response to the Schrems II judgment:

- Two redundant message processing platforms have been implemented in the Frankfurt data center located within the EU. The default regionalized setup encompasses micro-services and databases necessary for autonomous product processing and monitoring logging systems.

- Personal data stored on these platforms can only be accessed by Infobip’s authorized staff in the EU and countries with adequate data protection.

- A dedicated customer support team for the EU Region-Locked Data Center has been created. Our internal organization has been redesigned and adjusted to provide customers with top-level support quality, including 24/7 support in the EU.

- Our cloud is now hosting these two platforms and we have a current list of sub-processors involved in this data center available here.

Simply put, using the EU Region-Locked Data Center means our customers can rest assured that their end-users’ personal data are stored and backed up in the EU and accessed from the EU and adequate countries.

Supporting customers in their compliance with Schrems II judgment

As part of the Schrems II alignment project, we have revised and upgraded our current technical, security, and organizational measures to ensure the utmost standard of compliance in communication service provisioning.

---

2 Exceptionally and only for purpose of complex troubleshooting when using E-mail or Voice product customer support might be provided by Infobip’s team from Bosnia and Herzegovina (following a transfer impact assessment and implementation of supplementary measures). In this exceptional case access will be temporary, and only to a limited set of data necessary to resolve the troubleshooting. Our team will resolve the troubleshooting only by accessing customer data on its original location without transferring it into another jurisdiction and is performed in a secure way enabled by strong authentication measures and access protocols according to Infobip Group security policies. For more information click here.
The following measures have been implemented to ensure the confidentiality, integrity, and availability of personal data: technical, security, and organizational measures.

Technical and security measures

1. Encryption

We support modern cryptographic algorithms aligned with relevant leading practices in cryptography (such as the National Institute of Standards and Technology (NIST) Special Publication 800-175B). This alignment ensures that information is protected with the most efficient cryptographic controls, considering the state of the information and the system or a system component that processes, transmits, or stores the data. Infobip ensures and implements:

   Encryption at-rest:
   - Message content encryption: AES-256
   - Transparent disk encryption: AES-256
   - Backup archives encryption: AES-256.

   Encryption in-transit:
   - HTTPS (Hypertext Transfer Protocol Secure) - web interfaces
   - IPsec VPN (Virtual Private Network) – establishment of secure tunnels
   - SMPP (Short Message Peer-to-Peer) over SSL/TLS – secure
   - SFTP (Secure File Transfer Protocol) - fast file transfer.

2. Comprehensive access control management system

We've applied security controls that govern people and processes logging across the entire program stack throughout the company, including but not limited to the following:

- Appropriate access mechanisms control access to information systems.
- All-access privileges are assigned based on the least privilege principle/need-to-know basis per the job responsibilities. Only employees with legitimate business justifications are granted administrative rights. Standard personal accounts, used for everyday activities, do not have administrative privileges.
- Access to privileged information is regulated through a formal approval process and is subject to continuous monitoring by automated systems.
- Segregation of duties is enforced at various levels (e.g., system administrators that manage corporate networks do not manage cloud-service environments dedicated to customers, and vice-versa).
- Infrastructure for internal corporate usage is appropriately segregated from the environments hosting customer services. The production and integration/testing environments are also physically and logically separated.
- Access to infrastructure levels is restricted to EU and EEA employees to maintain authorized data processing locations and prevent cross-border transfers.

Numerous technical security controls are implemented on an appropriate technology layer, following the principles of security-by-design and defense-in-depth.
Organizational measures and information security processes

Information security is organized using the Information Security Management System (ISMS) framework. The Management Board provides strategic objectives and resources for establishing ISMS, while the Chief Information Security Officer (CISO) and Corporate Security Department execute and manage ISMS objectives. The Chief Privacy Officer (CPO) manages control objectives management related to privacy and protection of personal data, which is executed by the Corporate Privacy Department.

Policies and procedures play a crucial role in achieving specific goals within the domains of information security and privacy. Roles and responsibilities are structured and appointed to avoid conflicting duties.

We implement and maintain a comprehensive information security program aligned with numerous globally recognized information security standards and frameworks. External audits and attestations confirm the program’s maturity on a regular basis for:

- ISO 9001:2015 Standard
- ISO/IEC 27001:2013 Standard
- ISO/IEC 27017:2015 Standard
- SOC2 Type 1 Report.

Our information security efforts are guided and monitored by the Chief Information Security Officer (CISO) and a dedicated Corporate Security Department composed of professionals that cover all areas of information security at the state-of-the-art level: SOC, Security Operations, Application Security, IT Security, Development Security Operations, Anti-Fraud, Business Continuity, Security and Security Governance.

Data Recovery test

Business continuity is crucial in today’s world where downtime is unacceptable. Infobip’s Business Continuity Program ensures uninterrupted delivery of our essential products and solutions during disruptions. The disaster recovery strategy for our EU Region-Locked Data Center is running live activities at both locations so that actions can continue at the other in the event of a disruption at one site. EU Region-Locked Data Centers are physically and logically separated data center facilities and can process all traffic independently. We have conducted disaster recovery testing and will continue to do so to ensure the commencement of business as usual during unforeseen events and provide our client’s assurance in the timely recovery of EU Region-Locked Data Centers.

How can you start using the EU Region Locked Data Center?

For more information on how to start using our EU region-locked data center and the commercial aspects of this service:

- current customers and partners should contact their account manager
- others can contact us via https://www.infobip.com/contact and when describing the communication goals within the form please indicate your interest in EU region-locked data center.