Lattice's Approach to EU Data Transfer Compliance post-*Schrems II*

Last Updated: October 15, 2020

At Lattice, we deliver best-in-class performance management software to some of the most demanding human resources and people operations teams in the world. We understand that compliance is not an option, and that for many of our product ambassadors, platform administrators, and loyal users, their jobs depend on our continued compliance with our regulatory obligations. With this in mind, Lattice constantly monitors the regulatory landscape for new developments and compliance best practices, including the practical effects of the recent decision from Europe's highest court, the European Court of Justice (CJEU), on international data transfers from the EU.

We know that some of our customers have questions about how the ruling affects their use of Lattice products. The purpose of this page is to address some of those concerns.

What did the CJEU recently decide regarding data transfers from the EU?

On the 16th July 2020, in a landmark decision (*Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, "*Schrems II*"), the CJEU invalidated the EU-US Privacy Shield Framework, one of the more common international transfer mechanisms relied up by US companies to receive EU data. At the same time, the court upheld the validity of the Standard Contractual Clauses ("SCCs"), another transfer mechanism.

However, while the SCCs continue to provide a valid transfer mechanism to transfer personal data out of the EU, the CJEU further explained that the data importer and data exporter may, in addition to the SCCs, need to agree appropriate supplemental measures (also referred to as "additional safeguards") to ensure an adequate level of protection for the transferred data in light of national security laws that may conflict with any such guarantees provided under the SCCs. The CJEU did not specify what these additional safeguards may entail, leaving much uncertainty in the legal landscape.

The court observed that as a whole, US law provides greater protections than EU laws in the area of redress for unlawful governmental processing of personal data, but for two problematic investigatory tools, E.O. 12333 and FISA Section 702, both of which grant U.S. governmental agencies with broad access to data transfers outside of the narrow data processing requirements of the GDPR. Accordingly, there is no procedural action (contractual, regulatory, or otherwise) that can completely remedy the conundrum. Fortunately, the U.S. government and EU have committed to working together to find an acceptable resolution to this issue.

In the meantime, Lattice will continue to closely-monitor the evolution of international data transfer mechanisms under the GDPR and emerging guidance to determine whether it will need to make any additional changes to its practices, including implementing any additional supplemental measures as a data importer.

Does Data Hosting in the EEA Provides Any Relief?

We are aware that certain data protection authorities have espoused the position that the only way U.S. businesses can comply with the court's ruling in Schrems II is to on-shore and host all EU personal data within the European Economic Area ("EEA"). This interpretation of the ruling lacks foundation in the text of the opinion or practical application of the law, for the following reasons:

- With respect to EU-US data transfers, the CJEU took issue solely with two regulatory mechanisms by which the U.S. government may obtain access to EU citizen personal data from U.S.-based processors. U.S.-based processors are within the reach of all U.S. Federal laws, including E.O. 12333 and FISA Section 702, *regardless of where the data is hosted*. Hosting data in the EEA provides no protection against the problematic form of U.S. governmental access and intrusion described in *Schrems II*.
- As a practical matter, unless a company's production data is hosted in the EEA *and never accessed by an overseas employee or worker*, hosting in the EEA accomplishes very little with respect to GDPR compliance. As soon as one U.S.-based person accesses a customer's production database from overseas, the entire production database technically is accessible and is deemed to have been 'exported' under GDPR.
- As a related practical matter, it is not financially viable for most international software-as-a-service (SaaS) businesses to support an entirely self-contained and fully localized business unit (development, sales, customer experience and support) within the EEA. Even most EU businesses rely on geographically distributed support teams to provide 'round the clock' customer support.
- The foregoing considerations remain regardless of the GDRP transfer mechanisms upon which SaaS vendors and their customers rely: Model Clauses, BCRs, or lawful derogations.

How Risky are Transfers of Data Pursuant to the SCCs for Lattice's Processing Operations?

Although it is ultimately for our customers (the data exporters) to make this determination, in Lattice's view, transfers of EU customer data to Lattice in the United should be regarded as low risk.

A U.S. Department of Commerce White Paper provides a detailed explanation of U.S. privacy law as it relates to government access to data, which Lattice customers can, in combination with the information provided on this page, use to independently complete their assessment of the data transfers it makes to Lattice and to reach the determination they need to make about Lattice as their US data processor.

To summarize some of the helpful commentary provided in the White Paper:

- Most U.S. companies do not deal in data of any interest to the U.S. intelligence agencies. Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data. Accordingly, Lattice has no basis to believe U.S. intelligence agencies would seek to collect its data.
- Parties to commercial contracts may undertake independent protective actions and corresponding analysis to ensure compliance with the GDPR. Several specific mechanisms are offered as examples.

What Actions Has Lattice Taken to Comply with International Data Transfer Requirements to Comply with the GDPR in Light of Schrems II?

Since the landmark ruling, Lattice has implemented a number of measures that aim to ensure an adequate level of protection for European data our customers transfer to Lattice for processing in United States and to ensure minimal disruption to our customers.

Specifically, Lattice has (and will continue) to implement the following measures:

- In addition to incorporating the SCCs, our customer Data Processing Addendum also enumerates our commitments to security, confidentiality of processing, limitations on international transfers of personal data, cooperation with data subject rights, notice of security incidents, and more.

- We have updated our DPA to provide greater contractual protections against law enforcement requests. In particular, Lattice contractually commits to redirect to the customer any government requests for their data (e.g. E.O. 12333 or FISA 702 orders) and commits to providing advance written notice of any compulsory requests to access their data, unless prohibited by law from doing so.

- We maintain a robust security and privacy program that addresses the management of security and security controls employed by Lattice. However, to give you a summary of some of the important and specific technical and organizational measures we have implemented (and will continue to implement) to safeguard against unauthorized access to our customers' data:

  (1) ***Encryption*****:** Lattice commits to protect the confidentiality of its customer data, in transit and at-rest, using the most secure forms of encryption available, including: SSH, TLS, and encryption and hashing protocols approved by NIST.

  (2) ***Access controls***: Lattice restricts third-party access to its internal tooling and infrastructure. Our Legal team evaluates all requests for access, and ensures that the request is appropriate for the work to be performed, and that the third-party follows all security and privacy provisions outlined in their contract. Once approved, Lattice only grants access through controlled accounts to clearly -defined portions of the system.

- Lattice does not sell, rent, or trade customers' personal data. When Lattice accesses data hosted in the EU, it is in service to our customers, such as: to provide our customers 24/7 technical support for their most critical issues, to deliver the right security solutions or to optimize their experience.

Lattice's executive leadership will continue to embrace, support and endorse the policies and recommendations proposed by its Information Security Management System (ISMS) Committee, including the regular review and assessment of all security systems and policies to ensure they meet or exceed industry best practices.

Over the coming months, we anticipate the EU supervisory authorities will issue additional guidance on how to comply with the new legal landscape after the Schrems II decision, including what the

supplementary measures could consist of. In addition, the current form of the SCCs were written before GDPR went into effect and may be due for an official revision; we continue to keep a close eye on forthcoming guidance to stay up to date.

Questions?

Lattice remains committed to maintaining the highest levels of privacy and security for our customers, and will continue to drive enhancements to our data protection safeguards. If you have any questions, please contact us at privacy@lattice.com.