

Schrems II Judgment FAQs External Version – July 2020

This document is a broad overview of the Schrems II judgment and does not provide legal advice. We urge you to consult with your own legal counsel to discuss the requirements applicable to your specific situation.

Introduction

This set of FAQs highlights the key topics addressed in [the Schrems II judgment \(the “Schrems II Judgment”\) from the Court of Justice of the European Union](#) (“CJEU”) to help our customers, partners and vendors understand Mastercard’s approach to the Schrems II Judgment.

What is the Schrems II Judgment?

On 16 July 2020, the CJEU handed down its judgment in the Schrems II case that has a major impact on international data transfers. The CJEU examined whether two data transfer mechanisms – i.e. the standard contractual clauses approved by the European Commission (“SCCs”) and the EU-US Privacy Shield – adequately protect EU personal data transferred to countries outside of the European Economic Area (“EEA”) that are not considered to ensure an adequate level of protection.

The CJEU invalidated the EU-US Privacy Shield while maintaining the validity of Standard Contractual Clauses (SCCs). Before using SCCs, companies should however conduct a detailed assessment of all circumstances of the transfer and implement additional safeguards as needed.

The Schrems II Judgment did not address the validity of Binding Corporate Rules, which continue to a valid legal transfer mechanism under the EU General Data Protection Regulation (“GDPR”).

Why is it important?

The Schrems II Judgment is a historic court decision that has significant impact on any company handling and transferring EU personal data – regardless of whether they are based in the EU or not. Companies will be expected to take on increased responsibility to protect EU personal data when transferred abroad and will be subject to heightened scrutiny from EU privacy regulators and consumer organizations.

We anticipate a period of legal uncertainty and further discussion on how to comply with the judgment in practice.

Can Mastercard continue to transfer EU personal data to the US?

Mastercard’s Binding Corporate Rules reflect the highest data protection standards in the EU and our BCRs have not been impacted by the Schrems II Judgment.

Mastercard has [Binding Corporate Rules \(BCRs\)](#) in place for all our activities involving EU personal data. Our BCRs have been approved by the EU privacy regulators and are recognized as a valid data transfer mechanism under the GDPR. There is therefore no immediate impact on Mastercard’s transfers of EU personal data, i.e. from EEA-based companies (e.g. customers) to Mastercard, and between Mastercard entities.

Importantly, [Mastercard's BCRs](#) set out a robust process approved by the EU privacy regulators for (i) handling government data access and law enforcement requests, and (ii) enabling EU individuals to exercise their rights and obtain compensation, wherever their data is located.

While we do not use the EU-US Privacy Shield, Mastercard relies on the SCCs to transfer EU personal data to its suppliers located outside of the EEA. Therefore, Mastercard will continue to monitor regulatory developments related to the SCCs and take appropriate actions.

How are Mastercard's BCRs impacted by the Schrems II Judgment?

The Schrems II Judgment did not impact the validity of binding corporate rules as a lawful transfer mechanism under the GDPR. There is therefore no immediate impact on Mastercard's BCRs, and no impact on Mastercard's transfers of EU personal data, i.e. from EEA-based companies (e.g. customers) to Mastercard, and between Mastercard entities. However, Mastercard will continue to monitor regulatory guidance and take actions accordingly.

What steps Mastercard will take to ensure compliance with the Schrems II Judgment?

Mastercard will continue ensuring adherence to the strong privacy commitments we made in our BCRs. In addition, Mastercard will be conducting in-depth assessment on our transfer of EU personal data to our suppliers located outside of the EEA which rely on SCCs, and take appropriate actions to mitigate any risks arising from the Schrems II Judgment.

What steps Mastercard will take to support its customers and partners?

Mastercard customers do not need to take immediate action as a result of the Schrems II Judgment to continue using our services. Mastercard's BCRs adduce adequate safeguards under the GDPR for Mastercard's customers and partners to transfer their EU personal data to Mastercard. Therefore, Mastercard will continue ensuring all its entities globally comply with our BCRs in relation to transfers of EU personal data outside of the EEA.

What steps Mastercard will take with its suppliers located outside of the EEA?

Mastercard relies on the SCCs to transfer EU personal data to suppliers located outside of the EEA. In addition, Mastercard has imposed key GDPR terms to the majority of our non-EEA suppliers, as part of our strong commitment to privacy and data protection globally. Mastercard will continue monitoring regulatory guidance and take necessary actions.

What is Mastercard's approach to the GDPR?

Mastercard has a long-standing commitment to privacy, data protection and information security.

We agree with the tenets of the GDPR that people have the right to understand how their personal data is handled and they should have control over their data.

Mastercard has taken the GDPR as an opportunity to review all our products, services and processes and ensure compliance with the new requirements. Going further, we have extended key protections of the GDPR to all individuals globally, and we have launched consumer-centric [Data Responsibility principles](#) that guide all our data practices.

We will continue to work with our customers, partners and vendors to assist them comply with their obligations under the GDPR. By working together, we can move forward with confidence, and continue to deliver innovative solutions worldwide that are privacy-compliant as well as safe and secure.

For more information about Mastercard's privacy practices as well as our Data Responsibility Imperative, please visit:

<https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy.html>