Privacy & Data Protection

BREXIT- Data Transfers
FAQs External – January 2021

This document sets out Mastercard's approach to data transfers following the UK leaving the EU ("Brexit") and does not provide any legal advice. We urge you to consult with your own legal counsel to discuss the requirements applicable to your specific situation.

Introduction

These FAQs aim to help our customers, partners and vendors understand Mastercard's approach to data transfers following Brexit. The EU-UK Trade and Cooperation Agreement ("Agreement") was agreed on 24 December 2020. The Agreement includes a transition period of up to six months for data protection matters. During this period, the European Commission ("EC") is expected to complete its adequacy assessment of the UK's data protection laws. During the transition period, personal data can continue to be transferred from the EU to the UK without implementing additional safeguards.

How does Mastercard transfer EU personal data from the European Economic Area ("EEA") to the UK?

Mastercard relies on its Binding Corporate Rules ("BCRs"), which were approved by all EEA regulators, to transfer EU personal data to Mastercard entities outside of the EEA in compliance with the EU General Data Protection Regulation ("GDPR"). This means that Mastercard considers it has adequate safeguards in place for our customers to transfer EEA personal data to Mastercard and for Mastercard to transfer this personal data to Mastercard entities outside of the EEA under the GDPR. Mastercard BCRs apply when Mastercard transfers or receives EEA personal data as data controller or data processor. In addition, Mastercard closely monitors European regulatory guidance which may require companies, including Mastercard, to update their BCRs. Given the above, Mastercard's ability to transfer personal data from the EEA to the UK should not be impacted by the EC's adequacy assessment.

How does Mastercard transfer EEA personal data to third parties outside of the EEA?

Mastercard relies on Standard Contractual Clauses ("SCCs") to transfer EU personal data to third party sub-processors outside of the EEA, including those located in the UK. This means that Mastercard has adequate safeguards in place to transfer EU personal data to third party sub-processors under the GDPR. Given this, Mastercard's ability to keep data flowing from the EEA to the UK would not be impacted by the EC's adequacy assessment. That said, like other companies, Mastercard will begin to update our SCCs, including adding additional safeguards as deemed necessary, as soon as the final version of the updated SCCs are published by the EC.

What about the transfer of personal data from the UK to the EEA?

We understand that the UK recognises all EEA countries as providing an adequate level of protection for personal data. Given this, Mastercard's ability to transfer personal data from the UK to the EEA should not be impacted by the EC's adequacy assessment. In addition, companies that rely on BCRs approved prior to Brexit are now able to apply to the UK ICO for re-authorisation.

Can we expect any changes on the basis of Schrems II?

UK companies can continue to rely on SCCs for the transfer of UK personal data to sub-processors outside of the EEA. We will monitor the UK ICO's position on adopting the EC's updated SCCs and ensure we implement appropriate measures as soon as there is clarity. Please refer to our position on the Schrems II Judgment here.