EU General Data Protection Regulation ("GDPR") – FAQs
External Version - 16 March 2018

This document is a broad overview of the GDPR 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.

Contents

Introduction

This set of FAQs highlights the key themes of the General Data Protection Regulation ("GDPR") to help our customers, partners and vendors understand the new legal framework for protecting personal data in the European Union ("EU"). It describes the key requirements of the GDPR as well as Mastercard's approach to them

We will continue updating this document so please check back for new versions we publish on this site or with your regular Mastercard contact.

1. What is the GDPR?

In spring 2016, a new legal framework for collecting and processing personal data was adopted in the EU – the GDPR – which will enter into force on 25 May 2018. It introduces new and enhanced data protection requirements for companies.

2. Who does the GDPR apply to?

The GDPR applies to all companies operating in the European Economic Area ("EEA"- EU countries + Iceland, Liechtenstein and Norway) that process personal data of people based in the EEA. It also applies to non-EEA based companies offering goods or services to people based in the EEA and to those who monitor the behaviour of people based in the EEA.

Key Changes

3. What are the key changes under the GDPR?

The GDPR introduces several key changes to how companies can collect, use, share, store and transfer personal data. For instance:

- **Definitions**. The definitions of personal data and sensitive data have been expanded.
- **Consent**. The conditions for obtaining a valid agreement by a person to use his/her personal data are more rigorous.
- **Individuals' Rights**. It will be easier for people to ask an organization for access to their data, to correct it, move it or erase it.
- **Transparency**. Individuals must receive detailed information about how their data will be collected, used, shared, transferred and retained.
- **Privacy by Design**. Companies must embed privacy into the design of their products and services throughout the whole product development lifecycle.

- **Accountability**. Companies must document their data processing activities, data flows and compliance as well as their risk and impact assessments. In some cases, they have to appoint a data protection officer.
- **Processors and Sub-Processors**. Data processors have direct obligations and liabilities under the GDPR, and must be authorized by the data controller to use sub-processors.
- **Data Transfers**. Companies must implement a valid data transfer mechanism to transfer personal data outside of the EEA.
- **Contracts**. Contracts must include mandatory provisions and clarify roles and responsibilities of each party handling personal data.
- **Data breach**. Companies are required to notify data breaches to supervisory authorities within 72 hours of awareness and, in some cases, to affected individuals.
- **Sanctions**. If companies don't meet the obligations of the GDPR, they will face fines of up to 4% of their global annual turnover or EUR 20 million whichever is higher.

Consent

4. What is a valid consent under the GDPR?

To comply with the GDPR requirements, consent (or agreement by the person whose data is being used) must meet strict requirements it must be:

- **Clear, affirmative and unambiguous**. The individual must provide consent by way of a clear and affirmative action, such as ticking a box when registering for a service or tapping an "I Agree" button when using a mobile application.
- **Informed**. The individual must be aware of who is collecting the data and the purposes of the processing.
- **Clear and plain language**. Consent needs to be separate and not be hidden within the terms of a privacy notice or terms of use.
- **Specific**. Consent should be specific to the processing activity. Where there are multiple processing activities, consent may have to be given for each purpose.
- **Freely given**. Individuals must have a genuine free choice and must be able to refuse or withdraw consent at any time without detriment.

Individuals' Rights

5. What kind of requests might we receive from individuals under the GDPR?

Under the GDPR, people have enhanced rights about how their personal data is handled. Specifically, they have the right to:

- Access the personal data held about them.
- Object to certain types of processing, such as receiving marketing communications.
- Request correction and deletion of their personal data.
- Request the transfer of their personal data in a machine readable format to another company (data portability).

They are entitled to make these requests free of charge and the data controller must respond to the requests within one month subject to subject to various considerations before responding.

Transparency

6. What are the transparency requirements under the GDPR?

People must receive detailed information relating to the processing of their personal data. This is the responsibility of the data controller and companies usually inform individuals about how their personal data is processed via a privacy notice. The GDPR increases the amount of information that needs to be provided. It also requires providing information in a concise (e.g., a layered privacy notice), easily accessible (e.g., via a prominent link on a website) form using clear and plain language.

Accountability

7. What does Accountability mean under the GDPR?

It means that companies need to comply with the GDPR requirements and be able to demonstrate compliance.

Practically, there are many ways to demonstrate compliance, including:

- Adopting data protection policies

- Maintaining records of processing
- Appointing a data protection officer
- Conducting a data protection impact assessment for high risk activities
- Consulting with supervisory authorities if needed.

Data Transfers

8. What is Mastercard's approach to the GDPR data transfer rules?

The GDPR continues to restrict transfers of personal data outside of the EEA unless the third country has obtained an "adequacy decision" from the EU Commission or the receiving entity has a valid data transfer mechanism in place.

Mastercard has developed and implemented Binding Corporate Rules ("BCRs") which are an internal code of conduct that defines Mastercard's policy regarding privacy and international data transfers and has been recognized under the GDPR as a valid data transfer mechanism for both controllers and processors.

Mastercard's BCRs have been formally approved by the EEA data protection authorities. A copy of our BCRs is available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.

Contracts

9. Why do we need to update our contracts?

The GDPR requires mandatory provisions to be included in contracts with customers, partners and vendors. It also requires contractual parties to clarify their respective roles and responsibilities when handling personal data.

Data Breach

10. What is the new Data Breach notification obligation?

Data controllers are required to notify a breach of personal data to the lead supervisory authority within 72 hours of awareness, unless the breach is not likely to create risks for the people whose data has been breached. In addition, the personal data breach must be communicated to the affected individuals without undue delay where the breach is likely to create a high risk for them.

Data processors must communicate any breach to the data controller without undue delay, and must assist the data controller in complying with its notification obligations.

Mastercard and the GDPR

Mastercard is in the process of implementing the required changes to bring all its products and solutions in full compliance with the GDPR by May 2018.

In addition, we will assist our customers, partners and vendors with their obligations under the GDPR. By working together we can move forward with confidence, and continue to deliver innovative solutions worldwide that are safe, simple, and smart.

For more information on the GDPR, please contact us at:
privacyanddataprotection@mastercard.com

Last updated: 16 March 2018