Brazil General Data Protection Act ("GDPA") / Lei Geral de Proteção de Dados ("LGPD") – FAQs External Version – September 25, 2020

This document is a broad overview of the GDPA 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 Brazil General Data Protection Regulation ("GDPA") / Lei Geral de Proteção de Dados ("LGPD") to help our customers, partners, and vendors understand the new legal framework for protecting personal information in Brazil. It describes the key requirements of the GDPA as well as Mastercard's approach to them.

Mastercard's Approach to the GDPA

Mastercard has a long-standing commitment to privacy, data protection, and information security. We recognize that the GDPA establishes the first comprehensive data protection law in Brazil and ensures a level playing field for all companies doing business in Brazil.

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

Mastercard has taken the GDPA as an opportunity to review all our products, services, and processes and to ensure compliance with the new requirements.

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

We will continue updating this document, so please check back for new versions with your regular Mastercard contact.

1. What is the GDPA?

In August 2018, a new legal framework for collecting and processing personal information was adopted in Brazil – the GDPA – which entered into force on September 18, 2020. It introduces new and enhanced data protection requirements for companies.

2. Was the entry into force of the GDPA extended?

The Brazilian Congress and Executive recently took action intended to postpone the entry into force of the GDPA, but these efforts failed, and the GDPA entered into force on September 18, 2020. The enforcement date of GDPA penalties (e.g., fines and other sanctions) was extended by law to August 1, 2021. However, the pending formation of the Data Protection Authority (ANPD) has not been postponed or otherwise impacted. On August 27, 2020, the Executive published the Decree approving the regulatory structure of the ANPD and establishing its roles. Likewise, several members of the ANPD's National Data Protection Council have already been officially appointed.

In the face of this uncertainty, and as a part of our Commitment to Privacy, Mastercard worked towards compliance with the GDPA by August 15, 2020.

3. To whom does the GDPA apply?

The GDPA applies to all companies operating in Brazil that process personal information of people based in Brazil. It also applies to non-Brazil based companies offering goods or services to people based in Brazil, and to those who monitor the behavior of people based in Brazil.

Key Requirements

4. What are the key requirements under the GDPA?

The GDPA introduces several key requirements for how companies can collect, use, share, store, and transfer personal information. For instance:

- **Definitions**. The definitions of personal information and sensitive data are very broad.
- **Consent**. The conditions for obtaining a valid agreement by a person to use his/her personal information are very rigorous.
- **Individuals' Rights**. People have the right to ask an organization for access to their data, to correct it, move it, or erase it, in addition to other rights.
- **Transparency**. People 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.
- **Liability**. Data processors (*operadores*) have direct obligations and liabilities under the GDPA.
- **Data Transfers**. Companies must implement a valid data transfer mechanism to transfer personal information outside of Brazil.
- **Data breach**. Data controllers (*controladores*) are required to notify data breaches to the ANPD in a timely manner and, in some cases, to affected people.
- **Sanctions**. If companies do not meet the obligations of the GDPA, they will face fines of up to 2% of the company group's gross revenue in Brazil in the preceding year or R$ 50 million (USD 13 million), whichever is higher.

Consent

5. What is a valid consent under the GDPA?

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

- **Clear, affirmative and unambiguous**. People must provide consent by way of a clear and affirmative action, such as checking a box when registering for a service or tapping an "I Agree" button when using a mobile application.
- **Informed**. People must be made aware of who is collecting the data and the purposes of the processing.
- **Clear and plain language**. Consent needs to be separate and not 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**. People must have a genuine free choice and must be able to refuse or withdraw consent at any time without detriment.

Individuals' Rights

6. What kind of requests might a company receive from people under the GDPA?

Under the GDPA, people have rights related to how their personal information is handled. For example, they have the right to:

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

They are entitled to make these requests free of charge, and the data controller (*controlador*) must respond to the requests within 15 days subject to various considerations before responding.

Transparency

7. What are the transparency requirements under the GDPA?

People must receive detailed information relating to the processing of their personal information. This is the responsibility of the data controller (*controlador*), and companies usually inform people about how their personal data is processed via a privacy notice. The GDPA 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.

Mastercard has updated its Global Privacy Notice and other privacy notices, where we have a direct relationship with cardholders. We have adopted layered privacy notices and explained how we handle personal information in a clear and reader-friendly manner.

Accountability

8. What does Accountability mean under the GDPA?

It means that companies need to comply with the GDPA 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; and
- Consulting with the ANPD, if needed.

Mastercard has appointed a Data Protection Officer in Brazil, based in São Paulo.

Data Breach

9. What is the new Data Breach notification obligation?

Data controllers (*controladores*) are required to notify a breach of personal information to the ANDPD in a timely manner, if the breach is likely to create risks for the people whose data has been breached. In addition, the personal information breach must be communicated to the affected people in a timely manner, where the breach is likely to create a high risk for them.

Mastercard vendors who have or suspect that they may have suffered a data breach that may impact Mastercard must report it immediately to Mastercard's Security Operations Center at +1-636-722-3600.

More Information

10. Whom should I contact if I need more information about the GDPA or Mastercard's commitment to privacy?

Please contact us at: privacyanddataprotection@mastercard.com.

Last updated: September 25, 2020