EKATA DATA PROCESSING AGREEMENT (DPA)

FREQUENTLY ASKED QUESTIONS

Updated April 2022

*This document is provided for informational purposes **ONLY**. It is not intended to provide legal advice. Ekata urges its customer to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations.*

At Ekata, a Mastercard company, nothing is more important than the success of our customers and the protection of our customers' data. To support that mission, Ekata and Mastercard have established a comprehensive privacy and data protection program. We dedicate significant global resources to ensure compliance with applicable data protection laws and we have embedded privacy and data protection into the design of our products and services. We know you may have questions about Ekata's approach to privacy and the Data Processing Agreement ("DPA") that Ekata offers to its customers. To help you develop a better understanding of the Ekata DPA, we have created this FAQ to answer some of the most common questions we are asked. All defined terms used in this FAQ are as set out in the DPA.

For additional information about Mastercard International Incorporated and its affiliates' (collectively, "Mastercard") commitment to Privacy and Privacy Notice, please see here.

General

Does Ekata have an internal privacy program?

Yes, Ekata maintains an internal privacy policy and annual privacy training for all team members.

Does Ekata make a DPA available to its Customers?

Yes, Ekata offers a DPA to its Customers here. However, not all Customer agreements will utilize this DPA; use cases will vary. The DPA is an agreement that sets out the legal framework under which Ekata Processes Customer Data and Personal Data. The DPA is an addendum or exhibit to the Principal Agreement, i.e., a Master Services Agreement ('MSA'), etc., between Ekata and its Customer.

Why can't my organization use its own DPA?

The Ekata DPA is specific to Ekata's multi-tenant services and covers our processes in relation to these. For example, the DPA covers our processes around privacy-related notifications, audits, certifications, security measures, and sub-processing activities, all of which are aligned to the way in which Ekata's services and its multi-tenant infrastructure work. The Ekata DPA is also drafted to seamlessly interoperate with the MSA and other relevant Ekata and Mastercard agreements.

What is the scope of the DPA?

The covers Customers globally and sets out relevant legal obligations and commitments related to the processing of Customer Data and Personal Data. For ease of reference, it uses certain terminology from specific privacy and data protection laws, e.g., "Controller" and "Processor" from the European Union's General Data Protection Regulation ("GDPR") which are recognized globally.The DPA also includes a specific addendum to address the California Consumer Privacy Act ("CCPA"). There may be other addenda added to the DPA, as privacy regulations continue to evolve globally.

Does the DPA apply to my organization if we don't have offices in Europe?

Yes, the majority of the DPA applies to Customers regardless of their connection to the European Economic Area ("EEA"), Switzerland and the United Kingdom ("UK") (together, "Europe"). Most of the commitments in the DPA stem from general privacy requirements in all data protection laws globally and are not specific to European laws.

What are Ekata and the Customer's respective roles under the DPA?

Ekata acts as the Controller with respect to Personal Data submitted by Customers to Ekata's services. The Customer either acts as a Controller or a Processor of such Personal Data. This is set out in Section 2 ("Roles of the Parties") of the DPA.

Why does Ekata need to be a Controller under the DPA?

Ekata must control the purposes of means of the processing of Customer Data to support the ongoing improvement of Mastercard's ta products and enable full capability to return more consistent, reliable results for our customers.

Data Subject Requests

How does Ekata handle requests from Data Subjects?

Ekata responds to Data Subject requests to exercise rights granted to Data Subjects under EU Data Protection law and CCPA, as applicable.

Sub-processors

Does Ekata use Sub-processors?

An effective and efficient performance of Ekata's services requires the use of Sub-processors. These Sub-processors can include Affiliates of Mastercard, Ekata, and/or other third parties such as vendors or service providers. Ekata's use of Sub-processors may require the transfer of Customer Data to Sub-processors for purposes like hosting Customer Data, providing customer support, and ensuring the services are functioning properly.

Technical and Organizational Measures

What security measures are in place to protect Customer Data?

Ekata maintains appropriate technical and organizational measures to protect Customer Data. Please also see Ekata's dedicated Security page detailing our compliance certifications and approach to security, or Annex 1 to the DPA.

Security Breach Notification

How would Ekata notify its Customers in the event of a Personal Data Breach?

Ekata maintains security incident management policies and procedures, which are described in the applicable Security FAQ (available here). In Section 9.1 of the DPA (available here) Ekata commits to notify Customers without undue delay after becoming aware of a Personal Data Breach.

If your organization is impacted by a security breach, your organization's Security Contact(s) will be notified. Steps on how to create and maintain your Security Contact List are available here

European Data Transfers

What is a transfer mechanism under EU Data Protection Law?

Under EU Data Protection Law, Personal Data cannot be transferred outside of Europe unless (i) the importing country has been deemed adequate by the relevant governmental body; or (ii) the data exporter has appropriate safeguards in place to ensure that the Personal Data transferred is subject to an adequate level of data protection. The "appropriate safeguards" include transfer mechanisms such as standard data protection clauses (i.e., the Standard Contractual Clauses) and binding corporate rules.

Which transfer mechanisms does Ekata offer in its DPA?

Depending on the specific Services the Principal Agreement, Ekata may transfer data based on one of two independent transfer mechanisms:

- Binding Corporate Rules ("BCRs") - company-specific, group-wide data protection policies approved by data protection authorities to facilitate transfers of personal data outside of Europe within the Mastercard group; and
- Standard Contractual Clauses published in 2021 (the "SCCs") - legal contracts entered into between contracting parties who are transferring personal data outside of jurisdiction to countries that have not been deemed adequate.

Does the DPA include the SCCs?

Yes, Ekata has updated its DPA to incorporate the June 2021 SCCs.

What if I have additional questions not answered in this FAQ?

If you have additional questions, please contact your Account Manager.

Where can I find additional legal documentation and information about Ekata's services?

- Ekata's Privacy Notice can be found here.
- Ekata's DPA can be found here.
- Ekata's MSA, which incorporates the DPA, can be found here.
- Ekata has a dedicated Security page.