December 2018

Mastercard Binding Corporate Rules

External Version

Contents

I. Summary

Mastercard is a technology company in the global payments industry that connects Individuals, financial institutions, merchants, governments, public sector bodies, and businesses worldwide. We facilitate the processing of payment transactions permitting Mastercard cardholders to use their cards and other payment technologies at millions of merchants and allowing Individuals, financial institutions, businesses, public sector bodies and businesses to complete payments among themselves. Our network provides Individuals and businesses with a quick, convenient and secure payment method that is accepted worldwide. Our mission is to make payments safe, simple and smart.

To support that mission Mastercard has 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 take privacy and data protection seriously at Mastercard. We have a dedicated Privacy & Data Protection Team that is led by our Chief Privacy Officer who reports to our General Counsel. Our General Counsel is a member of Mastercard's Management Committee who reports to Mastercard's Chief Executive Officer.

Mastercard conducts the following types of data Processing activities:

- **Payment processing.** As a processor of payment transactions, Mastercard obtains and processes Personal Information about cardholders and other Individuals from customers (e.g., issuing financial institutions (issuers), acquiring financial institutions (acquirers), merchants, public sector bodies, partners (e.g., digital wallets) and other businesses) to facilitate payment transactions;

- **Direct-to-consumer services.** Mastercard collects and processes Personal Information of Individuals (e.g., name, email, telephone number, type of payment card) to provide services and programs directly to them, such as loyalty and rewards programs, digital wallets, cardholder services, marketing programs and promotions;

- **Customer management.** Mastercard collects and processes Personal Information of customers, merchants, suppliers and vendors (e.g., business contact information) to contact them, to manage business relationships and to offer support services; and

- **Employee management.** Mastercard collects and processes Personal Information of Employees (e.g., name, salary, benefits, education, work experience), including information about contractors or job applicants. The information is used to manage the employment relationship and job application process.

If you are an Employee, please consult the internal version of Mastercard BCRs, which is available on the company's Intranet. If you are a job applicant or a former employee, our Mastercard BCRs apply to the processing of your Personal Information, and some of the sections applicable to our Employees may also apply to the processing of your Personal Information. These sections are only available in the internal version of our BCRs. We will provide you with a copy of our internal Mastercard BCRs upon request if you e-mail us at BindingCorporateRules@mastercard.com.

For our "core" payment processing activities, Mastercard acts as Data Processor on behalf of our financial institutions, merchants, customers and partners. For other activities such as programs offered directly to Individuals or employment-related activities, Mastercard acts as Data Controller. Mastercard has established a comprehensive privacy and data protection program and applies a holistic approach whether we act as Data Processor or Data Controller.

Mastercard is committed to comply with EU Data Protection Law, in particular the GDPR (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC and replaced from time to time), as implemented into applicable national legislation.

Mastercard's Binding Corporate Rules ("BCRs") are part of our privacy and data protection program and are aimed at facilitating the transfer of Personal Information to and among Mastercard BCR entities worldwide in compliance with EU Data Protection Law. However, where the applicable legislation, for instance applicable national data protection law, requires a higher level of protection for Personal Information, it will take precedence over the BCRs.

Our BCRs cover data Processing activities where we act either as Data Controller or as Data Processor. Therefore, unless otherwise specified, the rules specified in our BCRs apply to both types of activities. Where applicable, we specify which of the rules apply only to activities for which Mastercard is a Data Controller or a Data Processor.

At Mastercard, Personal Information is:

Processed fairly and in a transparent manner

Processed only if Mastercard can rely on a valid legal ground

Protected with additional safeguards if it is considered to be Sensitive Information

Adequate, relevant and not excessive, kept accurate and up-to-date

Processed for specified and compatible purposes, and not retained unnecessarily

Processed in accordance with Individuals' rights

Only used for automated processing in compliance with the law

Processed using operational and technical safeguards

Only processed by Processors if adequate protections exist

Mastercard Europe SA, Chaussée de Tervuren 198A, 1410 Waterloo, Belgium, is the entity responsible for compliance with the BCRs in Europe. Mastercard Europe SA accepts liability for any breach of the BCRs caused by another Mastercard entity located outside of Europe, including any Data Processor or Sub-Processor used by Mastercard. The Data Protection Authority competent for the supervision of Mastercard Europe SA is the Belgian DPA.

In addition, Mastercard is subject to Banking Regulations and the oversight of the European Central Bank with the National Bank of Belgium acting as the lead overseer. The BCRs requirements are without prejudice to any separation of payment card scheme and processing entities required under Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

All Mastercard BCR Entities are bound to comply with the BCRs requirements by an Intra-group Agreement. The Privacy & Data Protection Team will ensure compliance with the BCRs under Senior Executive oversight as well as internal and external reviews and audits.

Individuals have the right to lodge a complaint with the Belgian DPA or with the Data Protection Authority of their country of residence, place of work or place of alleged infringement if they believe that the BCRs have been breached.

Please refer to Glossary for capitalized terms used in this document.

II. Duty To Respect The BCRs

The BCRs set the standards that Mastercard satisfies when processing Personal Information about Individuals either as a Data Controller or as a Data Processor.

Mastercard's BCRs are binding on all Mastercard BCRs Entities and on all Mastercard Staff Processing Personal Information as follows:

- The Mastercard BCRs Entities are bound by an Intra-group Agreement to respect the BCRs. The Mastercard BCR Entities that are covered by the BCRs and have signed Mastercard's Intra-group Agreement are listed in **Appendix 1**.

- The Mastercard Staff are bound by the BCRs via the employment agreement, the company Code of Conduct and various Mastercard policies and procedures.

III. What Do Our BCRs Cover?

Mastercard's BCRs apply to all Mastercard BCRs Entities that process Personal Information either as Data Controller or as Data Processor. Therefore, unless otherwise specified, the rules of our BCRs apply to both types of Processing activities. Where applicable, we specify which of the rules apply only to activities for which Mastercard is a Data Controller or a Data Processor.

1. Geographical Scope

Our BCRs cover all Processing of Personal Information, which is or was subject to EU Data Protection Law, and is conducted by Mastercard BCRs Entities worldwide, including the Processing of Personal Information that is transferred and processed by a Mastercard BCRs Entity outside of Europe and the Processing of Personal Information that was subject to EU Data Protection Law and is onward transferred from a country outside of Europe. Our BCRs apply to all Mastercard BCRs Entities worldwide; a list of countries where Personal Information may be transferred is attached in Appendix 1.

2. Material Scope

Our BCRs cover the Processing of Personal Information described in this section.

Mastercard receives most of its data when it processes payment transactions; however, we receive a limited number of Personal Information to process these payment transactions. When we process payment transactions, we typically receive the following Personal Information: the personal account number, the merchant name and location, the date, time and the total amount of the transaction. Except as otherwise indicated in the chart below, we do not receive the cardholder's name or other contact information. Nor do we receive information about the type of product or service that is purchased.

In addition to our core payment transaction processing activities, we also:

- offer some optional programs. If an Individual decides to participate (i.e., opts-in) in these optional programs, we may collect additional Personal Information such as the Individual's name and their email address. Individuals are provided with a privacy notice for these optional programs, which describes the type of Personal Information we collect and how we process it. In most situations, Personal Information collected in the context of online marketing programs is collected directly from Individuals. We keep the Personal Information collected in the context of optional programs segregated

from Personal Information processed for payment processing, unless otherwise specified in the program-specific privacy notice.

- offer debit payment and cheque processing services. When we process Personal Information for debit payment and cheque processing services, we may process additional Personal Information such as the Individual's name, information that relates to the financial institutions (e.g., sort code), any reference in a free text field, the Individual's signature, and in limited situations other unique identifiers.

In more detail, we process the following categories of Personal Information, depending on the type of services provided, whether we act as a Data Controller or a Data Processor, the purpose of the Processing and the categories of Individuals:

Mastercard's Role	**Purposes**	**Types of Personal Information**
Processor	Authorizing, clearing and settling transactions on behalf of our financial institutions, merchants, customers and partners.	Personal Information of **cardholders and other Individuals**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Additional information for debit payment and cheque processing services (e.g., financial institution sort code, account number, free text reference, Individuals' signature for cheque and other unique identifiers).
Processor	Supporting our customers' issuing and acquiring business.	Personal Information of **cardholders**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Contact information (e.g., name, postal or email address, phone number) as well as other information (e.g. date of birth, gender, government ID) as/when provided by cardholders (for card registration purposes), issuers and acquirers. • Additional information provided by cardholders or merchants (e.g., delivery address, product codes). Personal Information of staff at **financial institutions and merchants**, such as: • Contact information (e.g., business email address, business postal address, business telephone number, job title). • Where EU Data Protection Law applies to legal entities, Personal Information includes address of merchants, merchant category (e.g., airline) and ID numbers.
Controller	Cardholder dispute resolution.	Personal Information of **cardholders and other Individuals**, such as: • Data necessary for cardholder dispute resolution (e.g., personal account number, cardholder contact

Mastercard's Role	Purposes	Types of Personal Information
		information, merchant details, items purchased, information about the dispute, and other unique identifiers for payment and cheque processing services).
Controller	Accounting, auditing and billing.	Personal Information data of **staff at financial institutions, merchants, customers and partners**, such as: • Contact information of persons at financial institutions, merchants, customers and partners (e.g., business email address, business postal address, business telephone number, job title). • Where EU Data Protection Law applies to legal entities, Personal Information includes address of merchants, merchant category (e.g., airline) and ID numbers.
Controller	Managing customer relationships and financial reporting, including relationships with financial institutions, merchants, customers and partners.	Personal Information of **staff at financial institutions, merchants, customers and partners**, such as: • Contact information of persons at financial institutions, merchants, customers and partners (e.g., business email address, business postal address, business telephone number, job title). • Where EU Data Protection Law applies to legal entities, Personal Information includes address of merchants, merchant category (e.g., airline) and ID numbers.
Controller	Managing suppliers and vendors.	Personal Information of **staff at suppliers and vendors**, such as: • Contact information of persons at suppliers and vendors (e.g., business email address, business postal address, business telephone number, job title).
Controller	Marketing activities, including offers, sweepstakes, contests and promotions.	Personal Information of **consumers and website users (whether or not cardholders)**, such as: • Contact information (e.g., name, postal or email address, phone number). • Electronic identification data (e.g., username, password, security questions, IP address). • Data collected in the context of online marketing programs (e.g., personal characteristics, life habits, consumption habits, interests, geo-location data, and voice and image recordings).
Controller	Compliance with applicable laws, regulations and law enforcement requests.	Personal Information of **Individuals, cardholders and staff at financial institutions, merchants, customers and partners**, such as: • Data required for legal compliance (e.g., know your customer information for anti-money laundering compliance, responding to Individuals' requests).

Mastercard's Role	Purposes	Types of Personal Information
Controller or Processor depending on activity	Fraud, authentication, financial crime and risk management.	Personal Information of **cardholders and other Individuals**, such as: • Fraud related payment data (e.g., personal account number, date/time/amount of the transaction, name, merchant's details and location). • Biometric data for authentication purposes (e.g., photographs, voice, fingerprint). • Online fraud and authentication data (e.g., users' device IDs, users' details, browser information, online behaviour, users' interactions with the device). • Financial crime data (e.g., data about money laundering, terrorist financing, bribery, corruption and other unlawful activities). • Location data. • Fraud score, type of fraudulent activity and confirmed fraudulent activity. • Additional information for debit payment and cheque processing services (e.g., financial institution sort code, account number and other unique identifiers, free text reference, Individuals' signature for cheques). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.
Controller	Internal research, reporting and analysis	Personal Information of **cardholders and other Individuals**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.
Controller or Processor depending on activity	Providing products and services directly to Individuals, including rewards programs, eWallets, and prepaid services.	Personal Information of **cardholders**, such as: • Loyalty and rewards data (e.g., cardholder name, e-mail address, billing or shipping address, phone number, personal account number, transaction data). • e-Wallet registration data (e.g., cardholder name, e-mail address, billing or shipping address, personal account number, card expiration date, card verification code). • Prepaid registration data (e.g., cardholder name, e-mail address, phone number, billing or shipping address, personal account number, card expiration date, and card verification code). • Biometric data for authentication purposes (e.g., photographs).

Mastercard's Role	Purposes	Types of Personal Information
Controller or Processor depending on activity	Providing products and services directly to financial institutions, corporate clients, merchants, customers and partners, including statistical reports and tools, prepaid management services, customer service support.	Personal Information of **staff at financial institutions, corporate clients, merchants, customers and partners**, such as: • Contact information or identifying details of persons at financial institutions, corporate clients, merchants, customers and partners (including but not limited to business or personal email address, business or personal postal address, business or personal telephone number, job title, date of birth, country of origin, social media accounts and information, IP addresses). • Where EU Data Protection Law applies to legal entities, Personal Information includes address of merchants, merchant category (e.g., airline) and ID numbers. Personal Information of **cardholders and other Individuals**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Data received for cardholder support (e.g., data received at a call centre) or cardholder services (i.e., data to support emergency card replacement services). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.
Processor	Providing data analytics products and services to financial institutions, merchants, corporate clients and partners with their instructions.	Personal Information of **cardholders and other Individuals**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.
Controller	Anonymising data for the purposes of developing and providing data analytics products and services	Personal Information of **cardholders and other Individuals**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.

If you are an Employee, please consult the internal version of Mastercard BCRs, which is available on the company's Intranet. If you are a job applicant or a former employee, our Mastercard BCRs apply to the processing of your Personal Information, and some of the sections applicable to our Employees may also apply to the processing of your Personal Information. These sections are only available in the internal version of our BCRs. We will

provide you with a copy of our internal Mastercard BCRs upon request if you e-mail us at BindingCorporateRules@mastercard.com.

IV. How Do We Protect Personal Information?

Personal Information is key to Mastercard's business activities. For our business to function we must handle Personal Information with keen sensitivity to privacy and security standards in order to protect Personal Information on behalf of all the members of our global payment network. Our company is committed to the protection of Personal Information and to compliance with relevant laws.

Mastercard first and foremost complies with applicable data protection law. The Mastercard BCRs Entities comply with EU data protection principles both when we act as a Data Controller and where we act as a Data Processor. However, where applicable national data protection law requires a higher level of protection for Personal Information, it will take precedence over the BCRs.

- When we act as a Data Controller, we establish processes and procedures to ensure compliance with all requirements of EU Data Protection Law.

- Where we act as a Data Processor, we process Personal Information on behalf of the Data Controller and upon its instructions as provided in the Mastercard Rules or in a specific agreement between Mastercard and the Data Controller.

The following describes how we respect the principles of EU Data Protection Law, including how we cooperate with our customers to ensure respect of those principles:

1. Transparency & Fairness

The Mastercard BCRs Entities provide Individuals with clear information on how we process Personal Information.

Transparency is a key value at Mastercard. We provide Individuals with a number of online and offline privacy notices, including our Global Privacy Notice and program-specific privacy notices. All our privacy notices include, at the minimum, the information required by the GDPR (such as the identity and contact details of the controller and the Data Protection Officer, the purpose(s) of the Processing and related legal grounds, the categories data recipients, and data transfers), and a link to the BCRs.

Our BCRs inform Individuals about:

(i) the data protection principles we apply when processing Personal Information (Section IV),

(ii) the liability regime applicable to such Processing (Section VI);

(iii) their third party beneficiary rights with regard to such Processing and how to exercise those rights (Section VI.2).

All Individuals have the right to easily access the BCRs. A public version of the BCRs will be published on Mastercard's public website, and Mastercard BCRs will be available on Mastercard's intranet.

2. Legal Ground For Processing

The Mastercard BCRs Entities only process Personal Information if they can rely on one of the limited legal grounds provided by EU Data Protection Law.

When a Mastercard BCRs Entity acts as a Data Controller, our Privacy & Data Protection Team reviews Personal Information Processing operations and ensures that the Processing is based on a legal ground for processing Personal Information, including for example:

- Individuals have unambiguously given their consent to the Processing of Personal Information;
- The Processing is necessary for the performance of a contract to which the Individual is a party or in order to take steps at the request of the Individual prior to entering into a contract;
- The Processing is necessary for compliance with a legal obligation; or
- The Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the third party or parties to whom Personal Information is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Individual.

Where we act as Data Processor, we process Personal Information at the direction of the Data Controller who is responsible for ensuring a valid legal ground for the Processing.

3. Sensitive Data

The Mastercard BCRs Entities only collect Sensitive Data when absolutely necessary for the purpose of the Processing and if they can rely on one of the limited legal grounds provided under EU Data Protection Law.

Certain categories of Personal Information are Sensitive Data and receive a higher level of protection under EU Data Protection Law.

When a Mastercard BCRs Entity acts as a Data Controller, we process Sensitive Data only in limited circumstances, and will not process Sensitive Data unless the Processing is based on a legal ground for processing Sensitive Data, including for example:

- Individuals have given their explicit consent to the Processing;
- The Processing relates to Sensitive Data which is manifestly made public by the Individual;
- The Processing is necessary for the establishment, exercise or defence of legal claims by Mastercard;
- The Processing is necessary for the purpose of carrying out the obligations and specific rights of Mastercard in the field of employment law; or
- The Processing is necessary to protect the vital interests of the Individuals or another person where the Individual is legally or physically incapable of giving his or her consent.

4. Data Quality

The Mastercard BCRs Entities comply with the data quality principle.

When a Mastercard BCRs Entity acts as a Data Controller:

- The Mastercard BCRs Entities ensures that Personal Information is:
    - Kept up-to-date (data accuracy);
    - Adequate, relevant and not excessive in relation to the purpose for which the information was collected and processed (data minimization);
    - Not retained for longer than is necessary for the purpose(s) for which it was originally collected, unless legislation requires us to maintain it (limited storage periods).
- Our transaction processing system is designed to minimize the amount of Personal Information collected and for that purpose relies primarily on the personal account number (and not on other directly identifiable information).
- We have implemented a records retention policy that sets out the appropriate time periods for which the Mastercard BCRs Entities will retain data, including Personal Information, in accordance with applicable law.

When a Mastercard BCRs Entity acts as a Data Processor, it will cooperate with and assist the Data Controller to comply with EU Data Protection Law, in particular it will comply with requests from the Data Controller:

- To update, correct or delete Personal Information, and will inform all Mastercard BCRs Entities to whom the data have been disclosed of the required update, correction or deletion of the Personal Information.
- To delete or anonymize the Personal Information as of the date when there is no justification to the retention of the data in an identified format, and will inform all Mastercard BCRs Entities to whom the Personal Information have been disclosed of the required deletion or anonymization of the Personal Information.

The Mastercard BCRs Entity acting as a Data Processor will comply with the above requests unless legislation imposed upon the Mastercard BCRs Entity prevents it from returning or destroying all or part of the Personal Information, in which case it will protect the confidentiality of the Personal Information and will not actively process it anymore.

5. Purpose Limitation

Mastercard BCRs Entities only collect Personal Information for specified, explicit and legitimate purposes and do not further process it in a way incompatible with those purposes.

When a Mastercard BCRs Entity acts as a Data Controller, we ensure that Personal Information is collected and processed only for specific and legitimate purposes and that it is not further processed in ways incompatible with the purposes of the collection.

One of the ways Mastercard ensures compliance with this principle is by embedding privacy and data protection standards into the product development lifecycle. As part of our product development process, the Privacy & Data Protection Team reviews the collection and use of Personal Information on a case-by-case basis to ensure that the Processing is undertaken for

specific and legitimate purposes and is compatible with the purpose for which the Personal Information was collected. We embed these requirements into our technology wherever feasible to do so.

When a Mastercard BCRs Entity acts as a Data Processor, we comply with the following requirements:

- We only process Personal Information on behalf of the Data Controller and in compliance with its instructions, including with regard to transfers of Personal Information to a third country. If a Mastercard BCRs Entity cannot comply with the Data Controller's instructions, it will inform promptly the Data Controller of its inability to comply, if possible before the Processing takes place, and unless a law prohibits such notice on important grounds of public interest. Once the Data Controller is notified, it is entitled to suspend the transfer of Personal Information and/or terminate the contract.

- We take steps to return, destroy or fully anonymize the Personal Information of our customers, acting as Data Controllers, on the termination of the provision of services related to the data Processing, unless otherwise legally permitted to continue processing the data (in which case we will only process the data to the strict extent permitted by applicable law).

- We fully cooperate with our customers to assist them in their role as Data Controllers to fulfil their data protection compliance obligations in accordance with EU Data Protection Law.

- When we use our Sub-Processors, including internal Sub-Processors, we make sure they process the Personal Information in line with the instructions of our customers acting as Data Controllers.

6. Rights Of Individuals

The Mastercard BCRs Entities comply with Individuals' requests to exercise their rights under EU Data Protection Law.

When a Mastercard BCRs Entity acts as a Data Controller, we ensure that Individuals can exercise their right to:

- Access copies of Personal Information relating to them and receive some Personal Information in a structured, commonly used and machine-readable format to transmit it to another Data Controller;

- Obtain rectification or erasure of Personal Information relating to them or restriction of the Processing;

- Object, on grounds relating to their particular situation, to the Processing of their Personal Information;

- Object to the Processing of their Personal Information for the purpose of direct marketing.

Where we act as Data Processor, we require our customers to develop and implement appropriate procedures for handling Individuals' requests exercising their rights to access, rectify, or erase their Personal Information, restrict or object to the Processing of their Personal Information, or exercise their right to data portability. We do not reply to Individuals' requests to exercise their rights unless authorized or required to do so by our customers, but instead

transmit them to our customers. We cooperate and support our customers in responding to such Individuals' requests, and have implemented technical and organizational measures for that purpose.

7. Automated Decision Making

The Mastercard BCRs Entities comply with the restrictions applicable to automated decisions making under EU Data Protection Law.

When a Mastercard BCRs Entity acts as a Data Controller, we ensure that Individuals are not subject to a decision which produces legal effects or that similarly significantly affects them and which is based solely on automated Processing of Personal Information, including Processing intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, unless the Processing is:

- Necessary for entering into or performing a contract between the Individual and Mastercard;
- Authorized by a law requiring that measures be implemented to safeguard the Individual's legitimate interests.
- Authorized by the Individual who has provided his or her explicit consent to such Processing.

When the processing is based on Individuals' consent or is necessary for entering into or performing a contract, Mastercard will implement safeguards to protect Individuals' rights, freedoms and legitimate interest, at least the right to obtain human intervention, to express his or her point of view and to contest the decision.

8. Data Security

The Mastercard BCRs Entities implement appropriate technical and organizational measures to protect Personal Information.

Information security is at the heart of Mastercard's business model. Mastercard continuously innovates to make electronic payments even more secure. We have introduced chip and pin technology and more recently the digitization and tokenization of payment cards on electronic devices. Mastercard and its peers developed the industry standard for the protection of payment card data (Payment Card Industry PCI data security standards) that is used globally by all parties involved in processing card transactions, including financial institutions and merchants.

Mastercard has implemented and commits to maintain a comprehensive written information security program that complies with EU Data Protection Law, as well as all other applicable privacy, data protection and information security requirements, including U.S. banking safety and security standards. Mastercard is audited for compliance with those banking security standards by U.S. banking regulators on an annual basis. In addition, Mastercard's information security program is audited by an independent third party auditor on an annual basis in accordance with established audit standards (SSAE 16).

Mastercard commits to implement state-of-the-art measures to secure Personal Information. In particular, Mastercard's information security program includes appropriate technical, physical, administrative, and organizational measures and safeguards designed to:

- Ensure the security and confidentiality of Personal Information;

- Protect against anticipated threats or hazards to the security and integrity of Personal Information;

- Protect against any actual or suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure, acquisition, use or access or any other unlawful forms of Processing of any Personal Information transmitted, stored or otherwise processed.

These measures include the following controls:

- Access controls of persons;
- Data media controls;
- Data memory controls;
- User controls;
- Personal controls;
- Access controls of data;
- Transmission controls;
- Input controls;
- Instructional controls.

For situations where a Mastercard BCRs Entity acts as a Data Controller, Mastercard's information security program ensures a level of security appropriate to the risks represented by the Processing and the nature of the data, as well as the state of the art and cost of implementation of those safeguards. Our program is reviewed at least annually to ensure that it is responsive to new and emerging threats to security. Where Sensitive Data is processed, Mastercard implements enhanced security measures as appropriate to the heightened risks of the Processing. We also require our Data Processors or Sub-Processors to maintain strong information security safeguards.

Where we act as Data Processor, we implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing in accordance with the GDPR, in particular:

- We and our Sub-Processors assist the Data Controller in ensuring compliance with its obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the Processing and information available.

- We and our Sub-Processors comply with security obligations equivalent to those imposed on the Data Controller by EU Data Protection Law, in accordance with the Mastercard Rules.

In case of Personal Data Breach, all Mastercard BCRs Entities will notify without undue delay Mastercard Europe SA and Mastercard's Data Protection Officer, who will document the Personal Data Breach. We will notify a Personal Data Breach as follows:

- Where the Personal Data Breach is likely to result in a risk to Individuals' rights and freedoms, we will notify the competent Data Protection Authority.

- When the Personal Data Breach is likely to result in a high risk to Individuals' rights and freedoms we will also notify Individuals of the Personal Data Breach.

- When we act as a Data Processor, we inform the Data Controller without undue delay after becoming aware of any Personal Data Breach.

9. Onward Transfers

The Mastercard BCRs Entities only complete onward transfers to a Data Controller, a Data Processor or a Sub-Processor in compliance with the BCRs and the GDPR requirements applicable to Data Processors and Data Transfers.

A. Onward Transfers To Data Controllers And Data Processors

The following section applies when Mastercard acts as a Data Controller.

The Mastercard BCRs Entities only communicate Personal Information to: (1) another Mastercard Data Controller in compliance with the BCRs, including with the transparency requirements and purpose limitation principle; and (2) a non-Mastercard Data Controller located outside of Europe if it complies with EU Data Protection Law and with the legal requirements applicable to data transfers (in particular Articles 45, 46 and 47 of the GDPR) .

In addition, any Data Processor, including an internal Data Processor (i.e., a Mastercard BCRs Entity) and an external Data Processor (i.e., non-Mastercard entity or a Mastercard entity which is not bound by the Mastercard BCRs), who may receive or process Personal Information on behalf of a Mastercard BCRs Entity is subject to a rigorous due diligence process. The facts gathering and the security aspect of the diligence process is led by Mastercard's Corporate Security Team, in collaboration with the Privacy & Data Protection Team. The findings of the due diligence are reviewed by the Privacy & Data Protection Team to ensure that our Data Processors apply appropriate protections to the data and that Mastercard complies with the legal requirements applicable to Data Processors and data transfers (in particular Articles 28, 29, 32, 45, 46 and 47 of the GDPR). The result of the diligence process is documented in a report, which includes any required risk mitigation measures. The process is repeated on an annual basis.

In particular, the Privacy & Data Protection Team ensures that:

- Where a Mastercard BCRs Entity uses an internal Data Processor to process Personal Information on its behalf and under its instructions, the Processing takes place in accordance with the BCRs.

- Where a Mastercard BCRs Entity uses an external Data Processor to process Personal Information on its behalf, the external Data Processor is bound by way of a written agreement to comply with data protection obligations in accordance with Article 28 of the GDPR, including:

    - Process Personal Information only on behalf of and under the instructions of the Mastercard BCRs Entity which acts as the Data Controller;
    - Implement and maintain appropriate technical and organizational measures to protect Personal Information against unauthorized access or disclosure, including by way of a comprehensive written information security program. Having regard to the state of the art and the cost of their implementation, such measures ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Information to be protected.
    - Inform the Mastercard BCRs Entity if it cannot comply with its data protection obligations, when there is a Personal Data Breach, an information security incident, or when it receives requests from Individuals or from a public authority;

- Only transfer Personal Information outside of Europe in compliance with Articles 45, 46 and 47 of the GDPR;
- Only sub-contract the Processing of Personal Information with the prior written consent of the Mastercard BCRs Entity which acts as the Data Controller and under an agreement that imposes on the Sub-Processor the same data protection obligations as set out in the contract between the Mastercard BCRs Entity and the external Data Processor;
- Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Assist the Mastercard BCRs Entity to ensure compliance with its obligations pertaining to the security of the Personal Data, data protection impact assessments and related prior consultations;
- At the choice of the Mastercard BCRs Entity, delete or return the Personal Data to the Mastercard BCRs Entity after the end of the provision of the services;
- Make available to the Mastercard BCRs Entity information necessary to demonstrate compliance with its obligations under the agreement and inform the Mastercard BCRs Entity if, in its opinion, an instruction infringes EU Data Protection Law;
- Remain liable to the Data Controller for the performance of the external Data Processor's obligations.

B. Onward Transfers To Sub-Processors

The following section applies when Mastercard acts as a Data Processor.

The Mastercard BCRs Entities only use internal Sub-Processors (i.e., a Mastercard BCRs Entity) or external Sub-Processors (non-Mastercard entities) in accordance with the Data Controller's instructions and the informed general or specific authorization provided in the Mastercard Rules or the specific data processing agreement between the Data Controller and the Mastercard BCRs Entity.

When we use external Sub-Processors, we bind them via a written agreement to ensure that they comply with the same obligations as are imposed by the Mastercard BCRs on Mastercard, via the Mastercard Rules or the specific agreement between the Data Controller and the Mastercard BCR Entity acting as Data Processor.

When the Data Controller gives a general authorization to the Mastercard BCRs Entity to use Sub-Processors, the Mastercard BCRs Entity commits to provide the Data Controller with a list of Sub-Processors and to inform the Data Controller of any addition or replacement of a Sub-Processor in a timely fashion so as to give the Data Controller an opportunity to object to the change or to terminate the contract before the Personal Information is communicated to the new Sub-Processor, except where the service cannot be provided without the involvement of a specific Sub-Processor.

In addition, Mastercard complies with the following requirements when sub-processing Personal Information:

- Our internal Sub-Processors are bound to respect our BCRs and only process Personal Information in line with the instructions of the Data Controllers which are specified in the Mastercard Rules or in a specific agreement.

- The Privacy & Data Protection Team ensures that Mastercard BCRs Entities only use Sub-Processors when appropriate data protection guarantees are implemented in accordance with Articles 28, 29, 32, 45, 46, 47 of the GDPR, in compliance with the Data Controller's instructions and prior authorization and the requirements outlined above for agreements with external Data Processors.

10. Accountability

Where we act as Data Controller, we implement appropriate technical and organizational measures to ensure and to be able to demonstrate compliance with the BCRs, in particular:

- We carry out data protection impact assessments for Processing operations that are likely to result in a high risk to the rights and freedoms of Individuals and consult the relevant DPA, where required under EU Data Protection Law.

- We implement appropriate technical and organizational measures designed to implement data protection principles and to facilitate compliance with the requirements set up by the BCRs (data protection by design and by default).

When we act as a Data Processor:

- We make available to the Data Controller information necessary to demonstrate compliance with its obligations and allow for and contribute to audits as provided in our BCRs.

- We inform the Data Controller if, in our opinion, an instruction infringes EU Data Protection Law.

- We assist the Data Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs, such as data protection by design and by default.

Whether we act as a Data Controller or a Data Processor, we maintain a record of Processing activities and make it available to the relevant DPA upon request.

V. How Do We Ensure Privacy Compliance?

The Privacy & Data Protection Team is responsible to ensure compliance with the BCRs requirements under senior executive oversight. Mastercard has a global team of dedicated privacy, data protection and security professionals responsible for administering our privacy and data protection programs.

Mastercard provides regular privacy and data protection training and awareness to Mastercard Staff globally, and all Mastercard Staff are required to comply with Mastercard's data protection policies and procedures. Mastercard's privacy and data protection program is subject to regular internal and external reviews and audits.

1. The Mastercard Privacy & Data Protection Team

The Privacy & Data Protection Team is in charge of ensuring compliance with the BCRs requirement and is led by Mastercard's Chief Privacy Officer who is an Executive Vice President and reports directly to our General Counsel. Our General Counsel is a member of Mastercard's Management Committee which reports to Mastercard's Chief Executive Officer.

Mastercard ensures that the Privacy & Data Protection Team has enough human and financial resources to complete its tasks efficiently and in accordance with EU Data Protection Law. In

particular, the Privacy & Data Protection Team is composed of a network of qualified data professionals as well as privacy and data protection lawyers devoting 100% of their time to privacy and data protection law. They are located in Mastercard main offices worldwide, including in the U.S., Belgium, the UK and Singapore. Senior privacy & data protection lawyers are in charge of supervising and coordinating compliance with applicable data protection rules globally. They report to Mastercard's Chief Privacy Officer and are assisted by mid-level and junior privacy and data protection lawyers. The exact structure of the Privacy & Data Protection Team is subject to change as Mastercard business evolves rapidly. An organigram of the Privacy & Data Protection Team is available upon request.

The Privacy & Data Protection Team is responsible for ensuring that the Processing of Personal Information by the Mastercard BCRs Entities is legally compliant, as well as ethical. Accordingly, the team is responsible for:

- Supervising and implementing the BCRs;
- Ensuring compliance with the requirements of the BCRs;
- Updating the BCRs in compliance with internal governance procedures;
- Handling requests and complaints of Individuals in relation to the BCRs.

2. Senior Executive Oversight

Mastercard's commitment to privacy starts at the highest levels of the organization, with our Board of Directors, Chief Executive Officer, General Counsel, Executive Vice President Chief Data Officer, Executive Vice President Chief Privacy Officer and our Executive Vice President Chief Security Officer. Mastercard's Chief Privacy Officer is an Executive Vice President and reports directly to our General Counsel. Our General Counsel is a member of Mastercard's Management Committee which reports to Mastercard's Chief Executive Officer.

3. Data Protection Officer

Mastercard has appointed a Data Protection Officer ("DPO"), who monitors compliance with the BCRs and is responsible for the following tasks:

- Informing and advising Mastercard and Mastercard Staff in all matters related to the Processing of Personal Information and their obligations under EU Data Protection Law;
- Monitoring compliance with EU Data Protection Law and Mastercard's policies, including the assignment of responsibilities, awareness-raising and training of Mastercard Staff involved with the Processing of Personal Information and related audits;
- Providing advice regarding data protection impact assessments upon request;
- Acting as a contact point for Individuals in relation to all issues related to the Processing of their Personal Information and to the exercise of their rights under EU Data Protection Law;
- Cooperating with DPAs, for which he or she may act as a contact point.

The DPO has been provided with the necessary resources to carry out his or her tasks. He or she enjoys the highest management support for the fulfilment of these tasks and does not receive instructions in this regard.

4. Privacy and Information Security Officers

The Privacy & Data Protection Team is supported in certain jurisdictions by data protection lawyers and information security officers. In addition, we have appointed data liaisons and records champions globally, who sit in a variety of business and support functions, and who promote employee awareness about data protection, records retention and these BCRs. The Privacy & Data Protection Team also works closely with multiple teams around the globe, including the Corporate Security Team as well as the Information Incident Response and Records Retention teams, to ensure that our privacy and data protection program and these BCRs are effectively implemented.

5. Training & Awareness

Mastercard BCR Entities provide appropriate training on the BCRs to Mastercard Staff who have permanent or regular access to Personal Information, who are involved in the Processing of Personal Information or are involved in the development of tools used to Process Personal Information.

Mastercard's Privacy & Data Protection Team provides Mastercard Staff with engaging, relevant and up-to-date training about a variety of privacy and data-related topics, including Mastercard's policies and procedures as well as these BCRs. Mastercard's privacy training program is designed to provide Mastercard Staff with the knowledge, tools and resources they need to protect Personal Information and is tailored according to role, function, and access to Personal Information.

All Mastercard Staff are required to take a mandatory data protection course and the completion of the course is audited. Specialized training modules are also provided for Mastercard Staff in specific roles, functions or in specific jurisdictions. We use interactive methods to deliver training including videos, webcast programs, live fora and social activities to stress the importance of data protection and the role of our BCRs to all Mastercard Staff.

6. Control & Audit

Mastercard commits to conduct data protection audits on a regular basis or on specific request from the Privacy & Data Protection Team.

Mastercard commits to take the following actions to control compliance with EU Data Protection Law, including all the requirements of the BCRs, by:

- Carrying out audits for compliance on a regular basis both internally and by appointing external auditors where needed and upon request;
- Designating the internal audit team as the department responsible for carrying out internal audit, and the internal audit team and the Privacy & Data Protection Team as the department responsible to design the scope of each audit of the BCRs based on a risk-based approach and in relation to the particular risks presented at the time of the audit;
- Communicating the results of the audit to the internal audit team, the Data Protection Officer, the Privacy & Data Protection Team and the Mastercard Board;
- Ensuring that corrective actions take place based on the results of the audit;
- Providing the Belgian DPA, other competent DPAs and customers with the result of the audit report upon request and under the strictest confidentiality obligations;

- Allowing the Belgian DPA and other competent DPAs to verify compliance of any Mastercard BCR entity with EU Data Protection Law and the BCRs in accordance with applicable law, in particular in respect of the highest confidentiality requirements, and without creating risks for the security, integrity and confidentiality of Mastercard's payment network and of the global financial system; and

- Cooperating with DPAs with regard to any questions relating to the Processing of Personal Information by the Mastercard BCR Entities.

None of the above confidentiality requirements should limit the Belgian DPA's or other competent DPAs' ability to issue enforcement notice, in compliance with applicable law, where corrective action arising from the audit is ignored.

Where we act as Data Processor and subject to the strictest confidentiality obligations, we allow the Data Controller to request an audit of our data protection compliance program by external independent auditors, which are jointly selected by Mastercard and the Data Controller. The external independent auditor cannot be a competitor of Mastercard. Mastercard and the Data Controller will mutually agree upon the scope, timing, and duration of the audit. Mastercard will make available to the Data Controller the result of the audit of its data protection compliance program. The Data Controller must reimburse Mastercard for all expenses and costs for such an audit. In addition to the above, if the Data Controller requesting the audit is a competitor of Mastercard, Mastercard will be entitled, in cooperation with the jointly selected external auditor, to redact any commercially sensitive and confidential information from the audit report.

In addition, we bind our external Sub-Processors to: (1) provide Mastercard with the necessary information to help us verify the Sub-Processor's compliance with its data protection obligations; and (2) where necessary allow Mastercard to perform or order an on-site audit of the procedures relevant to the protection of Personal Information on behalf of our customers, acting as Data Controllers.

VI. Liability

1. Responsibility Of Mastercard BCR Entities

The Mastercard BCRs are enforced by all Mastercard BCRs entities in accordance with an Intra-Group Agreement. Each Mastercard BCRs Entity is responsible for complying with the BCRs.

In addition to the individual responsibility of Mastercard BCRs Entities, Mastercard Europe SA accepts responsibility and agrees to:

- Take the necessary action to remedy breaches of these BCRs caused by other Mastercard BCRs Entities located outside of Europe, and contractual breaches caused by Data Processors or Sub-Processors located outside of Europe.

- Pay compensation for any material or non-material damages incurred as a result of such breaches by a Mastercard BCRs Entity, a Data Processor or a Sub-Processor, unless Mastercard Europe SA can demonstrate that the damage could not be attributed to a Mastercard BCRs Entity, a Data Processor and a Sub-Processor.

Mastercard Europe SA confirms that it has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.

2. Third Party Beneficiary Rights

In situations where Mastercard acts as a Data Controller, Individuals have the right to enforce the BCRs as third-party beneficiaries, including:

- The data protection principles and Individual's rights (Section IV);
- The right to complain through the internal complaint mechanism (Section VIII.1);
- The right to lodge a complaint with a DPA and to seek judicial remedies and to claim compensation in Courts (Section VIII.2);
- The process for handling conflicts of law (Section IX);
- The duty to cooperate with DPAs (Section VIII.3);
- This section on liability.

Therefore, if a Mastercard BCRs Entity violates the BCRs, courts and DPAs in Europe will have jurisdiction and Individuals will have the rights and remedies against Mastercard Europe SA as if Mastercard Europe SA had committed the violation in the country in which Individuals are located (instead of the country of the Mastercard BCRs Entity outside of Europe).

When we act as Data Processor on behalf of customers, customers believing that our BCRs are not complied with have the right to enforce the BCRs against any Mastercard BCRs entity for breaches they caused and the right to seek a judicial remedy or claim compensation from Mastercard, including for breach of the BCRs caused by internal or external Sub-Processors. Moreover, customers have the right to enforce the BCRs against Mastercard Europe SA for breach of the BCR or of the data processing agreement by internal or external Sub-Processors.

In addition, in situations where Mastercard acts as a Data Processor, Individuals have the right to enforce the BCR as third-party beneficiaries directly against Mastercard where:

- The requirements at stake are specifically directed to Data Processors in accordance with the GDPR, in particular the duty to (i) respect the instructions received from the Data Controller, (ii) implement appropriate technical and organizational security measures, (iii) notify any Personal Data Breach to the Data Controller, (iv) respect the conditions to engage a Sub-Processor, (v) cooperate with and assist the Data Controller in complying and demonstrating compliance with the law, (vi) provide easy access to BCRs, (vii) grant a right to complain through an internal complaint mechanism, (viii) cooperate with the DPA; as well as requirements pertaining to (xi) liability, compensation and jurisdiction and (x) conflicts of law.

- They are not able to bring a claim against the Data Controller because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor has assumed the entire legal obligations of the Data Controller by contract of by operation of law, in which case the Individuals can enforce their rights against such entity. In those situations, Individuals have the right to enforce Sections II, IV.1, IV.10, VI, VIII.1, VIII.3 and IX and Appendix 1 of the BCRs against Mastercard Europe SA.

In the above scenarios, Individuals are entitled to:

- Lodge a complaint before the DPA of the EU Member State of his or her habitual residence, place of work or place of alleged infringement and take action against

Mastercard before the Courts where the Data Controller or Mastercard has an establishment or where the Individual has his or her habitual residence.

- Obtain compensation and to remedy breaches of the BCRs. Where Mastercard, acting as a Data Controller or a Data Processor, and another third party involved in the same Processing are found responsible for any damage caused by such Processing, Individuals are entitled to receive compensation for the entire damage directly from Mastercard and the other third party involved in the Processing.

- Obtain a copy of the public version of the BCRs, including its appendixes, and a copy of the Intra-Group Agreement (without any sensitive and confidential commercial information).

3. Burden Of Proof

Where Individuals or customers bring a claim or proceeding for a violation of the Mastercard BCRs and can demonstrate that they have suffered damage and establish facts which show that it is likely that the damage occurred because of a violation of the Mastercard BCRs or contractual breaches caused by Data Processors or Sub-Processors located outside of Europe, Mastercard Europe SA is responsible for proving that the Mastercard BCRs Entity outside of Europe, the external Data Processors and Sub-Processor were not responsible for the violation giving rise to that damage or that no violation occurred. Where Mastercard Europe SA is successful in proving that the Mastercard BCRs Entity outside of Europe, the Data Processor and the Sub-Processor are not responsible for the violation, Mastercard Europe SA may discharge itself from any responsibility.

VII. Updates To The BCRs

We may update our BCRs to reflect, for example, changes in our Personal Information practices, modifications of the regulatory environment or our company structure. We commit to report changes to our BCRs without undue delay to all Mastercard BCRs Entities and to the Belgian DPA, and where necessary, we will seek a new approval of the BCRs. However, in certain situations, we may update the BCRs, including the list of Mastercard Entities bound by the BCRs, without re-applying for an approval. In addition to the above, where we act as Data Processor and where a change affects the processing conditions, we will inform the Data Controller in a timely fashion so as to give the Data Controller the opportunity to object to the change or to terminate the contract before the modification is made.

VIII. How Can You Lodge A Complaint And Enforce The BCRs?

1. Internal Complaint Handling

We have implemented internal policies, processes and procedures to allow Individuals to exercise their rights and to manage complaints regarding our Personal Information practices, and these are overseen by the Privacy & Data Protection Team, Mastercard's top management and the Data Protection Officer.

In situations where Mastercard acts as a Data Controller:

- If an Individual or a customer has reasons to believe that a Mastercard BCRs Entity has not complied with the BCRs, they can lodge a complaint with the Data Protection Authority or the courts of their country of residence or directly with Mastercard.

- To lodge a complaint with Mastercard, Individuals can proceed in the following ways:

- E-mail us at: BindingCorporateRules@mastercard.com by including the term "BCRs" in the subject line; or
- Write to us at: Privacy & Data Protection Team, Mastercard Europe SA, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium.

- All complaints are handled by our Privacy & Data Protection Team, assisted by the Data Protection Officer, as follows:
  - We review the complaint and send an acknowledgement of receipt within ten (10) working days.
  - We then investigate the complaint and respond to it as soon as possible and within one month of receipt.
  - If the complaint is particularly complex, or given the number of complaints, Mastercard will provide an estimate of when the response will be provided to the complainant and in any event the response will be provided within three months of the receipt and will explain why it needs extra-time.

- If the complaint is upheld, Mastercard BCRs Entities take appropriate remedial measures as necessary to resolve the complaint and ensure compliance with the BCRs as appropriate.

- If an Individual is not satisfied with the response from the Privacy & Data Protection Team, that Individual can lodge a complaint with the competent Data Protection Authority or lodge a claim with a court of competent jurisdiction, preferably the Belgian DPA or the courts of Belgium.

Where we act as Data Processor, we strongly encourage Individuals to first seek to contact the relevant Data Controller. If we receive a complaint directly from an Individual, our Privacy & Data Protection Team will review the complaint and will forward it to the relevant Data Controller, unless the Data Controller has ceased to exist or became insolvent in which case the complaint is handled by Mastercard as described above.

2. Redress for Individuals

In addition to the internal complaint described above, Individuals can seek redress by: (1) lodging a complaint with a Data Protection Authority; and (2) seeking a judicial remedy or claiming compensation in court. Individuals are free to lodge a complaint with a Data Protection Authority, seek a judicial remedy or claim compensation in court regardless of whether they have first lodged a complaint with Mastercard.

To ensure the best possible cooperation and efficiency in relation to complaints, it is preferable that Individuals exercise their rights before the Belgian DPA or the courts of Belgium. However, this does not preclude them from their right to enforce the BCRs before the Data Protection Authority or the courts of the Individual's country of residence, place of work or place of alleged infringement.

When we act as Data Processor on behalf of customers, customers who believe that our BCRs are not complied with have the right to seek a judicial remedy or claim compensation from Mastercard, including for breach of the BCRs caused by internal or external Sub-Processors.

3. Duty of Cooperation

Mastercard BCR Entities will cooperate with requests, queries or complaints from Individuals, Data Controllers and Data Protection Authorities. Mastercard BCR Entities will follow the

recommendations of the Belgian DPA and other competent DPAs regarding the implementation of the BCRs.

IX. How Do We Handle Potential Conflicts Of Law?

Where local law is likely to prevent a Mastercard BCRs Entity from fulfilling its obligations under these BCRs and where complying with such local law is likely to have a substantial adverse effect on the guarantees provided by these BCRs, the matter is referred to the Privacy & Data Protection Team for resolution, and as required under applicable law to the Belgian DPA. Our Privacy & Data Protection Team reviews each matter on a case-by-case basis and documents it internally.

If we receive an access request for Personal Information by a law enforcement authority or state security body ("requesting agency"), the Privacy & Data Protection Team responds to the enquiry by informing the requesting agency about our limited data set. We also refer the requesting agency to the appropriate financial institution, which holds more comprehensive information about the relevant cardholder.

Where the requesting agency pursues the request, we ensure that it follows the required legal process for its country and jurisdiction, including any applicable privacy safeguards. If there is a question about the legitimacy or scope of the request, we challenge it. Only when we are satisfied that the legal process is valid and appropriate, and when we are convinced that the request does not prevent a Mastercard BCRs Entity from fulfilling its obligations under these BCRs and does not have a substantial effect on the guarantees provided by them, do we deliver the narrowest possible set of data required to be responsive to the request while ensuring data minimization.

If we do not manage to resolve the conflict of laws, the Privacy & Data Protection Team will use its best efforts to put the access request on hold for a reasonable delay in order to consult with the Belgian DPA on how to resolve it, unless otherwise prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Mandatory requirements of local law applicable to a Mastercard BCRs Entity, which are not massive, disproportionate, indiscriminate and do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 23 of the GDPR are in principle not in contradiction with Mastercard BCRs and thus do not require consultation with the Belgian DPA. However, in case of doubt, Mastercard will consult with the Belgian DPA.

When the suspension and/or notification are prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Mastercard will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible to the Belgian DPA, and be able to demonstrate that it did so. If despite having used its best efforts, Mastercard is not in a position to notify the Belgian DPA, it will provide general information on the requests (e.g., number of applications for disclosure, type of Personal Information requested, requesting agency if possible) to the Belgian DPA upon request or whenever needed.

In addition to the above, where a Mastercard BCRs Entity acts as Data Processor, we notify the Data Controller when local laws prevent the Mastercard BCRs Entity (1) from fulfilling its obligations under these BCRs and have a substantial adverse effect on the guarantees provided by these BCR, and (2) from complying with the instructions received from the Data Controller via the Mastercard Rules or the data processing agreement between Mastercard and the Data Controller. We do not notify Data Controllers if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law

enforcement investigation. The Data Controller is responsible for notifying its competent Data Protection Authority if applicable and as authorized under applicable law.

Appendix 1 Mastercard Entities Covered By The BCRs

Mastercard BCR Entities and Mastercard Staff are bound to respect the BCRs. At a high-level, Mastercard BCRs Entities are structured as follows:

- Mastercard Europe S.A., Waterloo, Belgium is the European headquaters of Mastercard.
- Mastercard International Incorporated is the global headquaters of Mastercard.
- All other entities are subsidiaries or affiliates of Mastercard Europe S.A., Waterloo, Belgium or Mastercard International Incorporated.

The following Mastercard BCR Entities have signed Mastercard's Intra-group Agreement:

The following list is accurate as of December 2018. For a fully updated list of entities please contact the Privacy & Data Protection Team at BindingCorporateRules@mastercard.com.

FOR EUROPE:		
Country	**Mastercard BCRs Entity**	**Contact Details**
Austria	Mastercard Europe S.A. Austria Representative Office, Austria	Mastercard Europe SA Wipplingerstraße 30/DG 1010 Vienna, Austria
Azerbaijan	Mastercard Europe SA Azerbaijan Representative Office, Azerbaijan	AZ1078, Baku City, Nasimi District, Hasan Aliyev, 4/189, Falez Plaza, 6th Floor
Belgium	Mastercard Europe S.A., Waterloo, Belgium	Chaussée de Tervuren 198A B-1410, Waterloo, Belgium
	HomeSend SCRL Belgium	Rue des Colonies 56, 1000 Bruxelles, Belgium
Bosnia & Herzegovina	Mastercard Europe S.A., Bosnia & Herzegovina Representative Office, Bosnia	BIH – Sarajevo 1 FRA Andela Zvizdovica Unitic Business Center, Building A Bosnia, Sarajevo
Bulgaria	Mastercard Europe S.A. Bulgaria Representative Office, Bulgaria	Boulevard Totleben, 53-55, Stolichna Municipality, Sofia BG-1506, Bulgaria
Croatia	Mastercard Europe S.A. Croatia Branch Office, Croatia	Zagreb Tower Radnicka cesta 80/8 10 000 Zagreb, Croatia
Czech Republic	Mastercard Europe S.A. Czech Republic Branch Office, Czech Republic	Palladium, Na Porici 1079/3a, 110 00 Prague 1, Czech Republic

Denmark	Mastercard Europe S.A. Denmark Branch Office, Denmark	Gammel Kongevej 1 Copenhagen, 1610 Denmark
Finland	Mastercard Europe S.A. Finland Branch Office, Finland	Etelaesplanadi 2, 3C/4D Krs. Helsinki, 00130 Finland
France	Mastercard France SAS, France	112, Avenue Kleber 75784 Paris Cedex 16 France
Greece	Mastercard Europe S.A. Greece Representative Office, Greece	23 Vasilissis Sofias Avenue 10674 Athens, Greece
Germany	Mastercard Europe S.A. Germany Representative Office, Germany	Unterschweinstiege 10, 60549 Frankfurt/Main Germany
Hungary	Mastercard Europe S.A. Hungary Representative Office, Hungary	Deak Ferenc Utca 5H – 1052 Budapest Hungary
Ireland	Eurocommerce Call Centre Solutions Limited, Ireland	Block C, Central Park, Dublin 18, Ireland
	Eurocommerce Internet Solutions Limited, Ireland	Block C, Central Park, Dublin 18, Ireland
	Mastercard Ireland Limited, Ireland	MountainView, Central Park, Dublin 18, Ireland
	Orbiscom Ireland Limited	MountainView, Central Park, Dublin 18, Ireland
Italy	Mastercard Europe S.A. Italy Branch Office, Italy	Piazza del Popolo 18, 1st Floor Roma, Italy - 00187
Israel	Mastercard Israel LTD	Aluf Kalman Magen 3, Tel Aviv, 6107075 Israel
Kazakhstan	Mastercard Europe S.A. Kazakhstan Representative Office, Kazakhstan	CDC 2 Business Centre,240v Furmanov Street, Almaty, Kazakhstan
Netherlands	Mastercard Europe S.A. Dutch Branch Office, Netherlands	Gustav Mahlerplein 105-115, 1082 MS Amsterdam, The Netherlands
	Mastercard Netherlands BV	Gustav Mahlerplein 105-115, 1082 MS Amsterdam, The Netherlands
Norway	Mastercard Europe S.A. Norway Branch Office, Norway	OSLO, Aker Brygge, 2nd Floor, Filipstads Brygge 1, Norway

Poland	Mastercard Mastercard Europe S.A. Poland Branch Office, Poland	Plac Europejski 1 Warsaw Spire, 31st Floor 00-844 Warsaw, Poland
Portugal	Mastercard Europe S.A. Portugal Representative Office, Portugal	Avenida Da Liberade 110, 1, Lisbon Portugal
Romania	Mastercard Europe S.A. Romania Branch Office, Romania	4-8 Nicolae Titulescu Street America House Building, West Wing, 2nd Floor 011141 Bucharest, Romania
Russia	Mastercard Europe S.A. Russia Representative Office, Russia	Entrance D, 4th floor, Tsvetnoy boulevard 2, 127051 Moscow Russia
	Mastercard OOO, Russia	Entrance D, 4th floor, Tsvetnoy boulevard 2, 127051 Moscow Russia
Serbia	Mastercard Europe S.A., Serbia Representative Office, Serbia	Vladimira Popovica 38-40, GTC 19 Avenue, 1st Floor, 11070 Belgrade, Serbia
Spain	Mastercard Europe S.A. Spain Branch Office, Spain	Paseo de la Castellana, 259 C, 11ª Torre Cristal / 28046 Madrid, Spain
Sweden	Mastercard Sweden Services AB	Kungsgatan 33, 4th Floor SE-111 56 Stockholm, Sweden
Switzerland	Mastercard Europe S.A. Switzerland Branch Office, Switzerland	Löwenstrasse 25 8001 Zürich
Turkey	Mastercard Europe S.A., Turkey Representative Office, Turkey	Tamburi Ali Efendi Sok., No: 1334337 Etiler – Istanbul
	Mastercard Payment Transaction Services Turkey Bilişim Hizmetleri A. Ş.	Ayazaga Mah. Mezarlik Sok., No: 3 Sanyer Istanbul, Turkey
UK	Mastercard Prepaid Management Services Limited, UK	Access House, Cygnet Road Hampton, Peterborough United Kingdom PE7 8FJ
	Mastercard Payment Gateway Services Limited, UK	10 Upper Bank Street London, E14 5NP United Kingdom
	Mastercard Payment Gateway Services Client Finance Limited, UK	10 Upper Bank Street London, E14 5NP United Kingdom

	Mastercard Track Ltd.	10 Upper Bank Street, London, E14 5NP
	Applied Predictive Technologies UK Ltd	70 Conduit Street 4th Floor London, UK W1S 2GF
	Mastercard UK Management Services Ltd, UK	19th Floor, 10 Upper Bank Street, London, E14 5NP
	Vocalink Holdings Limited	1, Angel Lane, 9th floor, London EC4R3AB, United Kingdom
	Vocalink Limited	1 Angel Lane, London, EC4R 3AB, United Kingdom
Ukraine	Mastercard Europe S.A. Ukraine Representative Office, Ukraine	17/52, Bogdana Khmelnitskogo Street Floor 4A, Office 404A Kiev, 01030, Ukraine
FOR NORTH AMERICA:		
Country	**Mastercard BCRs Entity**	**Contact Details**
Canada	Mastercard technologies Canada ULC	2 Bloor Street West, Suite 1400, Toronto, ON M4W 3E2, Canada
United States	Mastercard International Incorporated	2000 Purchase Street Purchase, NY 10577 U.S.A.
	Mastercard Technologies, LLC	2200 MasterCard Boulevard 63368-7263 O'Fallon, Mo UNITED STATES
	Mastercard International Services, Inc.	2000 Purchase Street, Purchase New York 10577
	Mastercard Advisors, LLC	100 Manhattanville Road, Purchase, New York 10577
	Mastercard Advisors, LLC Europe	100 Manhattanville Road, Purchase New York 10577-2509
	Orbiscom Inc.	2000 Purchase Street, Purchase, Harrison, NY 10577-2509
	The Corporation Trust Company	2000 Purchase Street, Purchase, New York 10577 U.S.A.
	Mastercard Mobile Transactions Solution, Inc.	2000 Purchase Street, Purchase New York 10577
	Mastercard Travelers Cheque, Inc.	2000 Purchase Street, Purchase New York 10577

	Truaxis, Inc.	959 Skyway Road, Suite 150, San Carlos, CA 94070, United States
	Applied Predictive Technologies (APT), Inc.	4250 N Fairfax Drive; 11th Floor; Arlington, Virginia 22203
	APT Software Holdings, Inc.	4250 North Fairfax Drive, 11th Floor, Arlington, Virginia, 22203, U.S.A.
	Brighterion, Inc.	150 Spear Street, 10th Floor, San Francisco, California 94105
FOR ASIA PACIFIC:		
Country	**Mastercard BCRs Entity**	**Contact Details**
Australia	Mastercard Loyalty Solutions Australia Pty Ltd	72 Christie Street, St Leonards NSW 2065, Australia
	APT Australia Pty. Ltd.	Level 13, 333-339 George Street , Sydney NSW 2000
India	Mastercard India Services Private Limited	4th Floor, DLF Plaza Tower, DLF Phase 1, Gurgaon – 122 002, India
	Mastercard Technology Private Limited, India	Business Bay, 10th Floor, Tower A, Wing 1 Survey No. 103, Opp. Poona Club Golf Course Airport Road, Yerwada, Pune – 411 006, India
	Mastercard Mobile Transactions Solutions Private Limited	Business Bay, 4th Floor, Tower A, Wing 1 Survey No. 103, Opp. Poona Club Golf Course Airport Road, Yerwada, Pune – 411 006, India
	Mastercard Loyalty Solutions India Private Limited	602-603, Windfall, Sahar Plaza, J B Nagar, Andheri-Kurla Road Mumbai, Maharashtra, 400 059 India
Japan	APT Japan G.K.	CERULEAN TOWER 16F 26-1 Sakuragaoka-cho Shibuya-ku, Tokyo 150-0031 Japan
Singapore	Mastercard Asia/Pacific Pte. Ltd, Singapore	3 Fraser Street DUO Tower, Level 17, Singapore 189352

FOR MIDDLE EAST & AFRICA:		
Country	**Mastercard BCRs Entity**	**Contact Details**
South Africa	Mastercard Payment Gateway Services PTY Limited, South Africa	The Apex Building, 4th floor, Cape Town, South Africa, 7441 South Africa
	5one Marketing SA Pty Ltd, South Africa	Regent Square, Cnr Doncaster Road & Rosmead Avenue, Kenilworth, 7708, South Africa

The Privacy & Data Protection Team will assess on a case-by-case basis the data transfer practices of any newly acquired companies that have not yet signed Mastercard's Intra-group Agreement and implement appropriate interim data transfer solutions, including contractual guarantees.

Appendix 2 Glossary

Data Controller – means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Information.

Data Processor – means the natural or legal person, public authority, agency or any other body which processes Personal Information on behalf of and under the instructions of the Data Controller.

Data Protection Authority or DPA – means the independent public authority supervising compliance with privacy and data protection legislation.

Employee – means past, present and prospective employees, consultants, temporary workers, independent contractors, directors or officers employed or hired by Mastercard.

EEA – means the European Economic Area, comprised of the EU Member States plus Iceland, Liechtenstein and Norway.

EU Data Protection Law – means: (1) the GDPR and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and their national implementing legislations; (2) the Swiss Federal Data Protection Act; (3) the Monaco Data Protection Act; (4) the Data Protection Acts of the EEA countries (all the above as amended and replaced from time to time).

Europe – means the EU Member States, EEA countries, Switzerland and Monaco.

GDPR – means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

Individual – means an identified or identifiable natural or legal person (to the extent a legal person is subject to national data protection law) to whom the Personal Information pertains.

Intra-group Agreement – means the intra-group agreement that binds Mastercard BCR Entities to the BCRs.

Mastercard – means the Mastercard Group composed of Mastercard International Incorporated, Mastercard Europe SA, their subsidiaries and affiliates.

Mastercard BCRs Entity(ies) – means the Mastercard entities that are bound by the BCRs and have duly executed the Intra-group Agreement (listed in Appendix 1).

Mastercard Rules – the Rules for the Mastercard, Maestro and Cirrus brands, as available at http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf.

Mastercard Staff – Employees, consultants, temporary workers, independent contractors, directors or officers employed or hired by Mastercard and who are bound by the BCRs.

Personal Data Breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.

Personal Information – means any information relating to an identified or identifiable natural or legal person (to the extent a legal person is subject to national data protection law), an identifiable natural or legal person is one who can be identified, directly or indirectly, in particular by reference to an identification number (such as the personal account number) or to

one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Processing – means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Sensitive Data – means any Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.

Sub-Processor – means the entity engaged by the Data Processor or any further sub-contractor to process Personal Information on behalf of and under the instructions of the Data Controller.