MASTERCARD BINDING CORPORATE RULES

Public Version

Mastercard Binding Corporate Rules

Public Version

Contents

I. Summary 3
II. Duty To Respect The BCRs 6
III. What Do Our BCRs Cover? 6
1. Geographical Scope 6
2. Material Scope 6
IV. How Do We Protect Personal Information? 9
1. Transparency & Fairness 10
2. Legal Ground For Processing 10
3. Sensitive Data 10
4. Data Quality 11
5. Purpose Limitation 12
6. Rights Of Individuals 12
7. Automated Decision Making 13
8. Data Security 13
9. Onward Transfers 14
A. Onward Transfers To Data Controllers And Data Processors 14
B. Onward Transfers To Sub-Processors 15
V. How Do We Ensure Privacy Compliance? 16
1. The Mastercard Information Governance & Privacy Team 16
2. Senior Executive Oversight 17
3. Data Protection And Information Security Officers 17
4. Training & Awareness 17
5. Control & Audit 18
VI. Liability 19
1. Responsibility Of Mastercard BCR Entities 19
2. Third Party Beneficiary Rights 19
3. Burden Of Proof 20
VII. Updates To The BCRs 20
VIII. How Can You Lodge A Complaint And Enforce The BCRs? 20
1. Internal Complaint Handling 20
2. Redress For Individuals 21
3. Duty Of Cooperation 21
IX. How Do We Handle Potential Conflicts Of Law? 22

Appendix 1 Mastercard Entities Covered By The BCRs 23
Appendix 2 Glossary 25

I. Summary

Mastercard is a technology company in the global payments industry that connects Individuals, financial institutions, merchants, governments and businesses worldwide. We facilitate the processing of payment transactions permitting Mastercard cardholders to use their cards and other payment devices at millions of merchants. 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 Information Governance & Privacy Team that is led by our Chief Information Governance & 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 from customers (e.g., issuing financial institutions (issuers), acquiring financial institutions (acquirers), merchants or partners (e.g., digital wallets)) 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 Employee 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 EU Data Protection Directive 95/46/EC (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 Informaiton

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 Privacy Commission.

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 Information Governance & Privacy 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 Privacy Commission or with the Data Protection Authority of their country of residence 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.

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 is 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?

Our BCRs cover the Personal Information Processing for which we act 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.

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 data elements to process these payment transactions. When we process payment transactions, we receive the following Personal Information: the personal account number, the merchant name and location, the date, time and the total amount of the transaction. However, 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 offer some optional programs. If an Individual agrees to participate (i.e., opts-in) in these 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.

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**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant).
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**, such as: • Data necessary for cardholder dispute resolution (e.g., personal account number, cardholder contact information, merchant details, items purchased, and information about the dispute).
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,	Personal Information of **staff at financial institutions, merchants, customers and partners**, such as: • Contact information of persons at financial institutions,

Mastercard's Role	Purposes	Types of Personal Information
	including relationships with financial institutions, merchants, customers and partners.	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 **cardholders and staff at financial institutions**, such as: • Data required for legal compliance (e.g., know your customer information for anti-money laundering compliance).
Controller or Processor depending on activity	Fraud and risk management.	Personal Information of **cardholders**, such as: • Fraud related data (e.g., personal account number, date/time/amount of the transaction, name and location of merchant, IP address, fraud score, location data). • Biometric data for authentication purposes (e.g., photographs).
Controller	Internal research, reporting and analysis	Personal Information of **cardholders**, such as: • Transaction data (i.e., personal account number, date/time/amount of the transaction, name and location of merchant).
Controller or Processor depending on activity	Providing products and services directly to Individuals, including rewards programs, eWallets,	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).

Mastercard's Role	Purposes	Types of Personal Information
	and prepaid services.	• 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).
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 of persons at financial institutions, corporate clients, 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. Personal Information of **cardholders**, 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 (e.g., data to support emergency card replacement services). • Any other information provided by financial institutions, corporate clients, merchants, customers and partners.

Our BCRs also cover the processing of our Employees Personal Information. 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 Employee 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 identity of the Data Controller, the purpose for which Personal Information is processed, how the information is transferred, and any further information necessary to make the Processing fair and transparent, including data recipients and Individuals' right to access and correct their Personal Information.

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 Information Governance & Privacy 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;
    - Adequate, relevant and not excessive in relation to the purpose for which the information was collected and processed;
    - Not retained for longer than is necessary for the purpose(s) for which it was originally collected, unless legislation requires us to maintain it.
- 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 information governance standards into the product development lifecycle. As part of our product development process, the Information Governance & Privacy 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. 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, in which case the Data Controller 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 data processing services, unless otherwise legally permitted to do so (in which case we will not actively process the data anymore).

- 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;
- Obtain rectification, erasure or blocking of Personal Information if it is incomplete or inaccurate;
- Object, on compelling legitimate grounds, 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, block or erase their Personal Information. We cooperate with our customers and support them in responding to such Individuals' requests.

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 significantly affects them and which is based solely on automated Processing of Personal Information intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, unless the Processing is:

- Conducted in the course of the entering into, or performing of, a contract provided the request for the entering into or the performance of the contract, lodged by the Individual, has been satisfied and that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view or get human intervention;
- Authorized by a law requiring that measures be implemented to safeguard the Individual's legitimate interests.

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 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 comply with security obligations equivalent to those imposed on the Data Controller by EU Data Protection Law, in accordance with the Mastercard Rules, and we inform the Data Controller in a timely fashion in case of an information security incident and do best efforts to remedy the situation as soon as possible.

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 EU Data Protection Law, in particular with Articles 16, 17, 25 and 26 of the EU Data Protection Directive 95/46/EC (or their equivalent under EU Data Protection Law as revised and replaced from time to time).

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 in particular with Articles 25 and 26 of the EU Data Protection Directive 95/46/EC (or their equivalent under EU Data Protection Law as revised and replaced from time to time).

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 Information Governance & Privacy Team. The findings of the due diligence is reviewed by the Information Governance & Privacy Team to ensure that our Data Processors apply appropriate protections to the data and in particular that Articles 16, 17, 25 and 26 of the EU Data Protection Directive 95/46/EC (or their equivalent under EU Data Protection Law as revised and replaced from time to time) are complied with. 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 Information Governance & Privacy 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, 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 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 16, 17, 25 and 26 of the EU Data Protection Directive 95/46/EC (or their equivalent under EU Data Protection Law as revised and replaced from time to time);
    - 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 ensure a level of protection of Personal Information equivalent to the written agreement between the Mastercard BCRs Entity and the external Data Processor.

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 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 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 Information Governance & Privacy Team ensures that Mastercard BCRs Entities only use Sub-processors when appropriate data protection guarantees are implemented in accordance with Articles 16, 17, 25 and 26 of the EU Data Protection Directive 95/46/EC (or their equivalent under EU Data Protection Law as revised and replaced from time to time), in compliance with the Data Controller's instructions and prior authorization and the requirements outlined above for agreements with external Data Processors.

V. How Do We Ensure Privacy Compliance?

The Information Governance & Privacy Team is responsible to ensure compliance with the BCRs requirements under senior executive oversight. Mastercard has a global team of dedicated information governance, privacy 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 Information Governance & Privacy Team

The Information Governance & Privacy Team is in charge of ensuring compliance with the BCRs requirement and is led by Mastercard's Chief Information Governance & 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 Information Governance & Privacy Team has enough human and financial resources to complete its tasks efficiently and in accordance with EU Data

Protection Law. In particular, the Information Governance & Privacy 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 Information Governance & Privacy Officer and are assisted by mid-level and junior privacy and data protection lawyers. The exact structure of the Information Governance & Privacy Team is subject to change as Mastercard business evolves rapidly. An organigram of the Information Governance & Privacy Team is available upon request.

The Information Governance & Privacy 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 Information Governance & Privacy Officer and our Executive Vice President Chief Security Officer. Mastercard's Chief Information Governance & 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 And Information Security Officers

The Information Governance & Privacy Team is supported in certain jurisdictions by data protection officers 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 Information Governance & Privacy 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.

4. 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 Information Governance & Privacy 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 is 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.

5. Control & Audit

Mastercard commits to conduct data protection audits on a regular basis or on specific request from the Information Governance & Privacy 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 Information Governance & Privacy 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 Information Governance & Privacy Team and the Mastercard's Board;
- Ensuring that corrective actions take place based on the results of the audit;
- Providing the Belgian Privacy Commission, other competent DPAs and customers with the result of the audit report upon request and under the strictest confidentiality obligations;
- Allowing the Belgian Privacy Commission and other competent DPAs to verify compliance 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 Privacy Commission'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

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 the 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 right to seek judicial remedies and to receive compensation. 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 if 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 I, II, IV, VI.3, VIII, IX, and Appendix 1 of the BCRs against Mastercard Europe SA, and to:

- Lodge a complaint before the DPA or Courts competent for the European Data Controller. If this is not possible because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent, the Individuals have the right to take action before the DPA or the court competent for Mastercard Europe

SA, and to lodge a complaint before the court of his place of residence. If more favourable solutions for the data subject exist according to national law, then they would be applicable.

- Obtain compensation and to remedy breaches of the BCRs.

- 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 to all Mastercard BCRs Entities and to the Belgian Privacy Commission, and where necessary, we will seek a new authorization for 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 authorization. In addition, 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 manage complaints regarding our Personal Information practices, and these are overseen by the Global Information Governance & Privacy Team and Mastercard's top management.

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: Global Information Governance & Privacy Team, Mastercard

Europe SA, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium.

- All complaints are handled by our Information Governance & Privacy Team 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 the sending of the acknowledgement of receipt.
    - If the complaint is particularly complex, 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 sending of the acknowledgement of receipt and will explain why it needs extra-time in the acknowledgement of receipt.
- 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 Information Governance and Privacy 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 Privacy Commission 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 Information Governance & Privacy 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.

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 Privacy Commission 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.

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 Privacy Commission 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 would have a substantial adverse effect on the guarantees provided by these BCRs, the matter is referred to the Information Governance & Privacy Team for resolution. Our Information Governance & Privacy 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 Information Governance & Privacy 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 Information Governance & Privacy Team will use its best efforts to put the access request on hold for a reasonable delay in order to consult with the Belgian Privacy Commission 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 do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13 (1) of Directive 95/46/EC (as amended and replaced from time to time, in particular by the General Data Protection Regulation), are in principle not in contradiction with Mastercard BCRs and thus do not require consultation with the Belgian Privacy Commission. However, in case of doubt, Mastercard will consult with the Belgian Privacy Commission.

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 Privacy Commission, 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 Privacy Commission, it will provide statistical information (e.g., number of requests, type of data requested) to the Belgian Privacy Commission on an annual basis 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. The following Mastercard BCR Entities have signed Mastercard's Intra-group Agreement:

The following list is accurate as of January 26, 2016. For a fully updated list of entities please contact the Information Governance & Privacy Team at BindingCorporateRules@mastercard.com.

FOR EUROPE:
Mastercard Europe S.A., Waterloo, Belgium; Mastercard Europe S.A. Austria Representative Office, Austria; Mastercard Europe S.A. Bulgaria Representative Office, Bulgaria; Mastercard Europe S.A. Croatia Branch Office, Croatia; Mastercard Europe S.A. Czech Republic Branch Office, Czech Republic; Mastercard Europe S.A. Denmark Branch Office, Denmark; Mastercard Europe S.A. Finland Branch Office, Finland; Mastercard Europe S.A. Germany Representative Office, Germany; Mastercard Europe S.A. Greece Representative Office, Greece; Mastercard Europe S.A. Hungary Representative Office, Hungary; Mastercard Europe S.A. Italy Branch Office, Italy; Mastercard Europe S.A. Dutch Branch Office, Netherlands; Mastercard Europe S.A. Norway Branch Office, Norway; Mastercard Mastercard Europe S.A. Poland Branch Office, Poland; Mastercard Europe S.A. Portugal Representative Office, Portugal; Mastercard Europe S.A. Romania Representative Office, Romania; Mastercard Europe S.A. Spain Branch Office, Spain; Mastercard Europe S.A. Switzerland Branch Office, Switzerland; Mastercard Europe S.A. Russia Representative Office, Russia; Mastercard Europe S.A. Ukraine Representative Office, Ukraine; Mastercard Europe S.A., Serbia Representative Office, Serbia; Mastercard Europe S.A., Turkey Representative Office, Turkey; Mastercard Europe S.A., Bosnia &Herzegovina Representative Office, Bosnia, Mastercard Europe SA Azerbaijan Representative Office, Azerbaijan; Mastercard Europe S.A. Kazakhstan Representative Office, Kazakhstan; Mastercard Payment Transaction Services S.A., Poland; 5one Marketing Limited, UK; Mastercard France SAS, France; Mastercard OOO, Russia; Mastercard Prepaid Management Services Limited, UK; Mastercard Payment Gateway Services Limited, UK; Mastercard Payment Gateway Services Client Finance Limited, UK; Applied Predictive Technologies UK Ltd; Eurocommerce Call Centre Solutions Limited, Ireland; Eurocommerce Internet Solutions Limited, Ireland; Mastercard Ireland Limited, Ireland; Mastercard UK Management Services Ltd; Orbiscom Ireland Limited; 5one Marketing Limited, UK; Mastercard Netherlands BV; Mastercard Europe Sweden Filial; HomeSend SCRL Belgium; Mastercard Payment Transaction Services Turkey Bilişim Hizmetleri A. Ş
FOR THE USA:
Mastercard International Incorporated; Mastercard Technologies, LLC; Mastercard International Services, Inc.; Mastercard Advisors, LLC; Mastercard Advisors, LLC Europe; Orbiscom Inc.; Access Prepaid USA, Inc.; Mastercard Mobile Transactions Solution, Inc.; 5one USA, LLC; Mastercard Travelers Cheque, Inc.; Truaxis, Inc.; Applied Predictive Technologies (APT), Inc.; APT Software Holdings, Inc.
FOR ASIA PACIFIC:
Mastercard Asia/Pacific Pte. Ltd, Singapore; Mastercard India Services Private Limited, India; Mastercard Technology Private Limited, India; APT Japan G.K.; Pinpoint Pty Ltd, Australia; APT Australia Pty. Ltd.

FOR MIDDLE EAST & AFRICA:
Mastercard Payment Gateway Services PTY Limited, South Africa; 5one Marketing SA Pty Ltd, South Africa.

The Information Governance & Privacy 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 European Union ("EU") Data Protection Directive 95/46/EC (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; (2) the Swiss Federal Data Protection Act (as amended and replaced from time to time); (3) the Monaco Data Protection Act (as amended and replaced from time to time); (4) the Data Protection Acts of the EEA countries (as amended and replaced from time to time).

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

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 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 the recording, alteration, transfer, blocking or erasure of Personal Information, including collection, organization, storage, adaptation, retrieval, consultation,

disclosure, dissemination or otherwise making available, alignment or combination, or destruction.

Sensitive Data – means any Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, judicial data and criminal convictions, 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.