BINDING CORPORATE RULES POLICY

CONTENTS

INTRODUCTION TO THIS POLICY

This Binding Corporate Rules Policy ("**Policy**") establishes Rakuten's approach to the protection and management of personal data globally by Rakuten group members ("**Group Members**") when processing that data.

"**Personal data**" means any data relating to an identified or identifiable natural person in line with the definition in the GDPR (defined below), where the data relates to past, present and prospective:

(a) Rakuten employees (including individual subcontractors, secondees, interns work, experience students, agents temporary and casual workers and their family members/emergency contacts);

(b) customers;

(c) merchants (businesses which sell on the Rakuten platforms. Merchants' personal data is personal data of merchants' employees and merchants' end users); and

(d) Contractors' and suppliers' (including supplier personnel).

"**processing**" means any operation that Rakuten performs on personal data, whether manually or by automatic means. The 'collection' 'use' and 'transfer' of personal data are all elements of the definition of processing.

"**Europe**" means the countries in the European Economic Area plus Switzerland.

"**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation).

"**controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**processor**" means the entity which processes personal data on behalf of the controller.

What does this Policy cover?

This Policy applies to all personal data processed by Rakuten, including personal data processed:

(a) in the course of customer and merchant management[1]; and

(b) which relates to Rakuten employees, contractors and suppliers.

Specifically, personal data processed under the Policy may include (but is not limited to):

- In relation to **Rakuten employees**, personal data including: name; personnel ID (company number, identifier information and system ID); employment type; date of hire; salary grade; date of birth; passwords; business contact information; personnel car registration; payroll deposit information (bank information); network connectivity information; information related to electronic business travel; expense

[1] "Merchants" include merchants' employees and merchants' end users.

reporting/accounting information, including credit card information; benefits data; car allocation data; competency assessments; dependant data; disciplinary action data; education data; emergency contact data; employee profile data; employment data; HR audit data; individual development plan; international service data; management positions; organisational data; pay data; performance data; position data; appraisal data; security data; skills data; succession planning data; tax data; training data; survey information and responses; CCTV recordings; access control information; images;

- In relation to **customers,** personal data including: name; contact information; date of birth; interests; occupation/employment; social media attributes; demographic information; marketing preferences; details of goods and services purchased or for which the individual is a prospective customer; information relating to sales; survey information and responses; images;

- In relation to **merchants' personnel**, personal data including: name; ID and password assigned by Rakuten; title; gender; date of birth; business contact information; manager/principal's title; information relating to sales and transactions; Rakuten training information; CCTV recordings; images;

- In relation to **merchants' end users**, personal data including: name; contact details; details of transactions for goods and services; end user ID and password; gender, and date of birth; marketing preferences;

- In relation to **suppliers**, personal data including: name; contact information; details of goods and services provided; training information; identifier information; CCTV recordings; access control information; images; background check information; security vetting information.

Rakuten transfers personal data for the following purposes such as facilitating the provision of services and contract performance, marketing activities, management of suppliers, managing human resources and data analytics.

Who must comply with this Policy?

Group Members must comply with and respect this Policy when processing personal data for their own purposes.

This Policy does not replace any specific data protection requirements that might apply to a business area or function.

This Policy and a list of Group Members indicating the countries to which personal data may be transferred are published on the website accessible at https://corp.rakuten.co.jp/privacy/en/bcr.html.

BACKGROUND AND ACTIONS

1.1 What is Data Protection Law?

Data protection law regulates how people's personal data should be used. Rakuten's processing of the personal data of customers, employees, merchants, subcontractors and suppliers is covered and regulated by data protection law. Although many countries in which Rakuten is present have data protection laws, Rakuten has based this Policy on the data protection laws of the European Economic Area ("**EEA**").

1.2 **How does data protection law affect Rakuten internationally?**

Data protection laws in some jurisdictions do not allow the transfer of personal data outside such countries unless appropriate safeguards are put in place to protect the personal data. For example, data protection laws in Europe do not allow transfers to countries that do not ensure an 'adequate' level of data protection. Some of the countries in which Rakuten operates are not regarded by European supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

Other countries where Rakuten is established have similar export restrictions for personal data under local law.

1.3 **What is Rakuten doing about it?**

Rakuten is committed to take proper steps to ensure that its use of personal data on an international basis is safe and, hence, lawful. The purpose of this Policy, therefore, is to set out a framework to satisfy the requirements of local law applicable to Rakuten to provide an adequate level of protection for all personal data used, collected and transferred between Group Members.

This Policy applies to all Group Members where those Group Members process personal data both manually and by automatic means when the personal data relates to customer, employee and merchant data.

This Policy applies to all Group Members and their employees worldwide and requires that Group Members who collect, use or transfer personal data comply with the Rules set out in clause 2 of this Policy together with the policies and procedures set out in the appendices in clause 3 of this Policy.

1.4 **Further information**

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you can contact Rakuten's Global Privacy Manager at the address below who will either deal with the matter directly or forward it to the appropriate person or department within Rakuten.

Attention:	Global Privacy Manager
Email:	rakuten-privacy@mail.rakuten.com
Address:	Rakuten Crimson House, 1-14-1 Tamagawa, Setagaya-ku, Tokyo 158-0094

The Global Privacy Manager is responsible for ensuring that changes to this Policy are notified to the Group Members and to individuals whose personal data is processed by Rakuten.

If you are unhappy about the way in which Rakuten has used your personal data Rakuten has a separate complaint handling procedure which is set out in Part 3, Appendix 4.

2. OBLIGATIONS

This Policy applies in all cases where a Group Member collects, uses and transfers personal data.

Clause 2 of this Policy is divided into three sections:

- **Section A** addresses the basic principles that a Group Member must observe when it collects, uses and transfers personal data.
- **Section B** deals with the practical commitments made by Rakuten to the supervisory authorities in connection with this Policy.
- **Section C** describes the third party beneficiary rights that Rakuten has granted to individuals under clause 2 of this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW AND LEGAL BASIS FOR PROCESSING

Rule 1A – Rakuten will first and foremost comply with local law where it exists.

As an organisation, Rakuten's objective is to comply with applicable legislation relating to personal data wherever the Group Member is located (e.g.: in Europe, the GDPR and the local laws implementing it as amended or replaced from time to time and in Singapore with the Personal Data Protection Act 2012) and will ensure that where personal data is collected and used it is done in accordance with the applicable local law. Where there is no local law or the local law does not meet the standards set out by the Rules in this Policy, Rakuten's position will be to process personal data adhering to the Rules in this Policy.

Rule 1B – Rakuten will ensure that, where required, a legal basis exists for its processing of personal data.

Rakuten will ensure that a legal basis for processing personal data exists where required. For example, where personal data is subject to European data protection law or this Policy, subject to any specific provisions of European or Member State law, Rakuten will only process that data where:

- Rakuten has obtained consent to the processing, and the consent meets the required standards under the GDPR;
- 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 before entering into a contract;
- the processing is necessary for compliance with a legal obligation to which Rakuten is subject where that legal obligation derives from either European law or the law of a European Member State;
- the processing is necessary in order to protect the vital interests of an individual;

- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Rakuten where that processing is set out either in European law or in the law of a European Member State to which Rakuten is subject; or

- the processing is necessary for the purposes of the legitimate interests pursued by Rakuten or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the individual to whom the processing relates.

RULE 2 – ENSURING TRANSPARENCY AND PURPOSE LIMITATION DATA

Rule 2A – Rakuten will explain to individuals, at the time their personal data is collected, how that data will be used and will only use personal data for those purposes which are known to the individual or which are within their expectations and are relevant to Rakuten.

Rakuten will ensure, that individuals are always told in a clear and comprehensive way (usually by means of a fair processing statement) how their personal data will be processed. The information to be provided shall include the following in accordance with applicable data protection law:

- the identity and contact details of the controller;

- the contact details of the data protection officer;

- information about the individual's rights to access, rectify, erase their personal data, restrict the processing of their personal data and object to the processing of their personal data, and how individuals can express their concern and exercise their right to data portability; information about the right to lodge a complaint with the supervisory authority;

- information about the legal basis of processing and information about the legitimate interests pursued by the controller;

- where processing of personal data is based on consent the individual's right to withdraw consent;

- from which source the personal data originates, and if applicable, whether it came from publicly available sources;

- whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract and whether the individual is obliged to provide the personal data and the consequences of failure to provide such personal data;

- the uses and disclosures made of their personal data (including the secondary uses and disclosures of the information);

- the recipients or categories of recipients of their personal data,

- the transfer of personal data to another jurisdiction on the basis of this Policy and how to obtain a copy of this Policy;

- the retention period or the criteria for determining that period; and

- the existence of automated decision making including profiling.

Rakuten will follow this Rule 2A unless there is a legitimate basis for not doing so consistent with the applicable law of the country from which the personal data was transferred (for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, legal proceedings, the protection of the individual or of the rights and freedoms of others, or where otherwise permitted by the relevant law).

If a Rakuten Group Member outside Europe receives a legally binding request from a public authority for personal data that has been transferred to it from a Rakuten Group Member in Europe, Rakuten will act in accordance with Rule 16C and will take all possible steps to ensure that any disclosures of the personal data by it to any public authority are not massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society and demonstrate to the relevant data protection authorities if requested to do so the steps it followed to deal with the request in accordance with this Policy.

If Rakuten wishes to use personal data for a different or new purpose, Rakuten will not further process that information in a way incompatible with the purpose for which it was collected unless the change of processing is permitted by the law of the European country from which the personal data was originally transferred.

In certain cases, for example, where the processing relates to special categories of personal data, the individual's explicit consent to the new processing may be necessary.

RULE 2B – PROMOTING PRIVACY THROUGH TECHNOLOGY

Rakuten will promote privacy friendly technology and services through the concepts of privacy by design and by default. Rakuten's technology will be designed to implement data protection principles in an effective manner and to integrate the necessary safeguards. Further, Rakuten will promote technical solution that allow for a privacy friendly default setting of its services where appropriate.

Rule 2C – Rakuten will assess the impact of any new processing activity involving personal data to which European law applies that is likely to result in a high risk to the rights and freedoms of individuals.

Where Rakuten does initiate new processing activities involving personal data, it will ensure that such processing activities conform to the requirements of the data protection law and especially the principles, in the European country from which the personal data was originally transferred in accordance with its data protection impact assessment process, as amended and updated from time to time.

RULE 3 – ENSURING ACCURACY, STORAGE LIMITATION AND DATA MINIMISATION

Rule 3A – Rakuten will keep personal data <u>accurate</u> and <u>up to date</u>.

In order to ensure that the personal data held by Rakuten is accurate and up to date, Rakuten actively encourages individuals to inform Rakuten when their personal data changes.

Rule 3B – Rakuten will only keep personal data for <u>as long as is necessary</u> for the purposes for which it is collected and further processed.

Rakuten will comply with Rakuten's internal policies and procedures regarding document and data retention as revised and updated from time to time.

Rule 3C – Rakuten will only keep personal data which is adequate, relevant and not excessive in relation to the purpose for which it is processed.

Rakuten will identify the minimum amount of personal data that is required in order to properly fulfil the purposes for which it is processed.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Rakuten will always adhere to its IT security policies.

Rakuten will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of personal data over a network, and against all other unlawful forms of processing. To this end, Rakuten will comply with the requirements in the security policies in place within Rakuten as revised and updated from time to time together with any other security procedures relevant to a business area or function.

Rule 4B – Rakuten will adhere to its data incident management and notification policies.

Rakuten will adhere to Rakuten's data incident management and notification policies (as revised and updated from time to time) which set out the process that Rakuten must follow to:

- notify the competent supervisory authority of a data incident;
- notify individuals of a data incident involving their personal data; and
- assess the circumstances in which such notifications may not be required.

Rule 4C – Rakuten will ensure that providers of services to Rakuten also adopt appropriate and equivalent security measures.

Group Members using processors, which have access to the personal data covered by this Policy, will adhere to Rakuten's due diligence process for the selection of the service provider, take steps to ensure that the processors have proportionate technical and organisational security measures in place to safeguard the personal data and will impose strict contractual obligations in writing on the processor, which provide:

(a) commitments on the part of the processor regarding the security of that personal data, consistent with those contained in this Policy;

(b) that the processor will act only on the Group Members' instructions when using that information.

(c) as provided for in Rule 6, such obligations as may be necessary to ensure that the commitments on the part of the processor reflect those made by the Group Member in this Policy and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals under applicable law in respect of transfers of personal data to a processor established in a third country.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – Rakuten will adhere to the Subject Access Request Procedure and will be receptive to any queries or requests made by individuals in connection with their personal data.

In some countries individuals are entitled under the local law to be supplied with a copy of personal data held about them (including information held in both electronic and paper records), together with certain other details such as their rights in relation to their personal data. This is known as the right of subject access in European data protection law. Rakuten will follow the steps set out in the Subject Access Request Procedure (see Appendix 1) when dealing with requests from individuals for access to their personal data and in doing so will deal with requests within the timeframe described in the Subject Access Procedure (within one month from receipt of a request or such other period as may apply as determined by the law of the country governing the subject access request.

Rule 5B – Rakuten will deal with requests to access, erase, rectify, complete or restrict personal data, for data portability or objections personal data to the processing of personal data in accordance with the Subject Access Request Procedure.

In some countries such as in Europe individuals are entitled under the local law to:

- request rectification, erasure, restriction or completion, as appropriate of their personal data which is shown to be inaccurate or incomplete;
- object to the processing of their personal data; and /or
- Exercise their right to data portability in relation to their personal data

Rakuten will follow the steps set out in the Subject Access Request Procedure in such circumstances.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR CROSS-BORDER TRANSFERS

Rule 6 – Rakuten will not transfer personal data to third parties outside Rakuten without ensuring adequate protection for the information in accordance with the standards set out by this Policy.

In principle, cross-border transfers of personal data to third parties outside the Group Members are not allowed without appropriate steps being taken, such as binding oneself to appropriate contractual clauses or obtaining the consent of individuals which will protect the personal data being transferred in accordance with the standards set out by this Policy.

RULE 7 – SAFEGUARDING THE USE OF SPECIAL CATEGORIES OF PERSONAL DATA

Rule 7A – Rakuten will only process special categories of personal data if it is absolutely necessary to use it.

Special categories of personal data means information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data or biometric data processed for the purpose of uniquely identifying a natural person and criminal convictions. Rakuten will assess whether special categories of personal data is required for the proposed processing and when it is absolutely necessary in the context of the business.

Rule 7B – Rakuten will only process special categories of personal data where the individual's explicit consent has been obtained unless Rakuten has an alternative legitimate basis for doing so consistent with the applicable law under which the personal data was collected.

In principle, individuals must explicitly consent to Rakuten processing their special categories of personal data unless Rakuten has another legitimate basis for doing so consistent with the applicable law under which the personal data was collected. This permission to use special categories of personal data by Rakuten must be genuine and consistent with local consent requirements.

RULE 8 – LEGITIMISING DIRECT MARKETING

Rule 8A – Rakuten will allow individuals to opt out of receiving marketing information.

All individuals have the data protection right to object at any time, free of charge, to the use of their personal data for direct marketing purposes. Rakuten will honour all such objections. In some countries, such as Europe, this includes the right to object to profiling to the extent that it is related to such marketing (and in this context 'profiling' means the automated processing of personal data to analyse or predict certain aspects about an individual such as their economic situation, personal preferences, interests or location).

RULE 9 – AUTOMATED INDIVIDUAL DECISIONS, INCLUDING PROFILING

Rule 9 – Rakuten will not take decisions about individuals based solely on automated processing of their personal data

No evaluation of, or decisions about, an individual which produces legal effects or similarly significantly affects them will be based solely on the automated processing (including profiling as defined in Rule 8A) of their personal data unless:

- The processing is conducted in compliance with European data protection law; and
- Rakuten has put in place measures to safeguard the legitimate interests of individuals (such as the right for an individual to be informed of the existence of such processing, to be provided with information about the logic involved and the significance and consequences of the processing, to obtain human intervention in the decision, and to express their point of view and contest the decision).

Rakuten will not take any decisions described in this Rule 9 based on special categories of personal data.

SECTION B: PRACTICAL COMMITMENTS

RULE 10 – COMPLIANCE

Rule 10 – Rakuten will have appropriate staff and support to ensure and oversee privacy compliance throughout the business.

Rakuten has appointed its Global Privacy Manager as the person to oversee and ensure compliance with this Policy including monitoring training and complaint-handling. The Global Privacy Manager is supported by Local Privacy Contacts and Regional Privacy Officers, who are assigned to oversee Group Members) and who report to the Global Privacy Manager. The Regional Privacy Officers are responsible for overseeing and enabling compliance with this Policy on a day to day basis.

Where the Regional Privacy Officers are based in Europe or Rakuten has designated data protection officers in Europe, Rakuten ensures the independence of such officers to fulfil tasks prescribed under the Policy and under local law.

RULE 11 – TRAINING

Rule 11 – Rakuten will provide appropriate training to employees who have permanent or regular access to personal data, who are involved in the collection of personal data or in the development of tools used to process personal data in accordance with the Privacy Training Requirements attached as Appendix 2.

RULE 12 – AUDIT

Rule 12 – Rakuten will comply with the Audit Protocol set out in Appendix 3.

RULE 13 – COMPLAINT HANDLING

Rule 13 – Rakuten will comply with the Complaint Handling Procedure set out in Appendix 4.

RULE 14 – COOPERATION WITH SUPERVISORY AUTHORITIES

Rule 14 – Rakuten will comply with the Co-operation Procedure set out in Appendix 5.

RULE 15 – UPDATING THE RULES

Rule 15 – Rakuten will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 6.

RULE 16 – ACTION TO BE TAKEN WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE POLICY

Rule 16A – Rakuten will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under the Policy or such legislation has a substantial effect on its ability to comply with the Policy, the Global Privacy Manager will be promptly informed unless otherwise prohibited by law.

Rule 16B – Rakuten will ensure that where there is a conflict between the legislation applicable to it and this Policy, the Global Privacy Manager will make a responsible decision on the action to take and will consult the competent supervisory authority in case of doubt.

Rule 16C – Rakuten will ensure that where it receives a legally binding request from a public authority for disclosure of personal data exported from Europe under this Policy, Rakuten will, unless prohibited from doing so by a law enforcement authority, put the request on hold and promptly notify the Group Member that exported the personal data, unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, in which case it 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, and be able to demonstrate that it did so.

If, in the above case, despite having used its best efforts, the Group Member is not in a position to notify the Group Member that exported the personal data, it will

provide to the CNPD on an annual basis general information on the requests it received. In any event, the Group Member that imported the personal data will take all possible steps to ensure that any disclosures of the personal data by it to any public authority are not massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS European data protection law states that the customers, employees and merchants whose personal data is processed in Europe by a Group Member (the "**Exporting Entity**") and transferred to a Group Member outside Europe (the "**Importing Entity**") must be able to benefit from certain rights to enforce the Policy as follows:

- **Complaints**: Individuals may make complaints to Rakuten Europe S.à r.l. and/or to European supervisory authority in the jurisdiction of the Exporting Entity in accordance with the Complaint Handling Procedure.
- **Proceedings**: Individuals can bring proceedings against Rakuten Europe S.à r.l.
- **Liability**: Individuals may seek appropriate redress from Rakuten Europe S.à r.l. including the remedy of any breach of this Policy by any Importing Entity and, where appropriate, receive compensation from Rakuten Europe S.à r.l. for any damage suffered as a result of a breach of this Policy by a Group Member in accordance with the determination of a court or other competent authority.
- Individuals also have the right to obtain a copy of the Policy and the intra-Group Agreement entered into by Rakuten in connection with the Policy.

In the event of a claim being made in which an individual has suffered damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of this Policy, Rakuten Europe S. à r.l. has agreed that the burden of proof to show that an Importing Entity is not responsible for the breach, or that no such breach took place, will rest with Rakuten Europe S.à r.l.

3. **APPENDICES**

APPENDIX 1

Subject Access Request Procedure

BINDING CORPORATE RULES POLICY OF RAKUTEN

Subject Access Request Procedure

1. INTRODUCTION

1.1 Data protection laws in some jurisdictions give individuals the right to be informed whether any personal data about them is being processed by an organisation. This is known in Europe as the "right of subject access." This Subject Access Request Procedure ("**Procedure**") sets out how Rakuten will deal with such requests.

1.2 This Procedure also sets out the other rights individuals have in relation to their personal data under European law and the law of other jurisdictions and how Rakuten will deal with requests to exercise such rights. These rights are the right to rectification, the right to erasure, the right to data portability, the right to restriction of processing and the right to object to processing of personal data.

1.3 All queries relating to this Procedure are to be addressed to the Global Privacy Office or where feasible to a local privacy contact.

2. PERSONAL DATA SUBJECT TO EUROPEAN LAW

2.1 Individuals whose personal data is collected and/or used in Europe by Rakuten, and transferred between Rakuten group members ("**Group Members**") benefit from the rights mentioned above and such requests will be dealt with in accordance with the terms of this Procedure unless the applicable European data protection law differs from this Procedure, in which case the local data protection law will prevail.

3. PERSONAL DATA OUTSIDE THE SCOPE OF EUROPEAN LAW

3.1 To the extent that the local laws of non-European Group Members contain similar rights to those mentioned above, such Group Members will deal with those requests in accordance with this Procedure unless it differs from the applicable data protection law, in which case the local data protection law will prevail.

4. INDIVIDUALS' RIGHT TO SUBJECT ACCESS

4.1 An individual making a subject access request covered by clauses 2 or 3 above to Rakuten is entitled to:

(a) be informed whether Rakuten holds and is processing personal data about that person;

(b) be given a description of the categories of personal data and the purposes for which it is being held and processed;

(c) the recipients or classes of recipients and their location to whom the information is, or may be, disclosed by Rakuten;

(d) the retention period or criteria to determine this period;

(e) the right to complain to a competent supervisory authority;

(f) the existence of automated decision-making, including profiling;

(g) if the data is not collected from the individual any available information as to their source;

(h) the existence of the right to rectification, erasure, restriction of processing of the personal data and right to object to such processing;

(i) where data is transferred to a third country the right to be informed about the use of Binding Corporate Rules as safeguards for the transfer; and

(j) communication in intelligible form of their personal data held by Rakuten and where requested a copy of this.

4.2 The request must be made in writing, which can include email or other electronic means.[2]

4.3 Rakuten must deal with a subject access request within one month of receipt of that request (or such other period as may be determined by the law of the country in which the personal data was collected. That period may be extended by two further months where necessary as permitted by applicable law, taking into account the complexity and number of the requests.

5. PROCESS

5.1 Receipt of a subject access request covered under this Procedure.

(a) If Rakuten receives any request from an individual for their personal data, this must be passed to the Global Privacy Office immediately upon receipt indicating the date on which it was received together with any other information which may assist the Global Privacy Office to deal with the request.

(b) The request does not have to be official or mention data protection law to qualify as a subject access request.

5.2 Initial steps

(a) The Global Privacy Office will make an initial assessment of the request to decide whether it is a subject access request that falls within the scope of this Procedure and whether confirmation of identity, or any further information, is required.

(b) The Global Privacy Office will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

6. EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

6.1 A subject access request may be refused on the following grounds:

(a) Where the subject access request is made to a European Group Member and relates to the use or collection of personal data by that Group Member, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located; or

(b) Where the subject access request relates to personal data used or collected by a European Group Member but the request does not fall within section 6.1(a) because it is made to a non-European Group Member to which the personal data has been transferred, if the grounds for withholding such personal data are consistent with

[2] Unless the local data protection law provides that an oral request may be made, in which case Rakuten will document the request and provide a copy to the individual making the request before dealing with it.

the data protection law within the jurisdiction from which the information was transferred; or

(c) if the personal data is held by Rakuten in non-automated form and is not or will not become part of a filing system; or

(d) where the personal data does not originate from Europe and (subject to the provisions of local applicable law) the provision of the personal data requires Rakuten to use disproportionate effort; or

(e) where the subject access request is made to a non-European Group Member in circumstances in which clause 3.1 applies, and if the refusal to provide the information is consistent with the law applicable to the Group Member that has collected and transferred the personal data.

7. RAKUTEN'S SEARCH AND THE RESPONSE

7.1 The Global Privacy Office will arrange a search of all relevant electronic and paper filing systems.

7.2 The Global Privacy Office may refer any complex cases to the Executive Director of the Legal Department for advice, particularly where the request includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

7.3 The information requested will be collated by the Global Privacy Office into a readily understandable format (internal codes or identification numbers used at Rakuten that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared by the Global Privacy Office which includes information required to be provided in response to a subject access request.

7.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

8. REQUESTS FOR RESTRICTION, ERASURE, RECTIFICATION OR OBJECTION TO PROCESSING OF PERSONAL DATA

8.1 If a request is received for the restriction, erasure, rectification, or objection to processing of an individual's Personal Data, such a request must be considered and dealt with as appropriate by the Global Privacy Office. A request may be refused in accordance with the applicable local law.

8.2 If a request is received advising of a change in an individual's personal data, such information must be rectified or updated accordingly if Rakuten is satisfied that there is a legitimate basis for doing so.

8.3 When Rakuten erases, anonymises, rectifies, restricts the processing or honours a request to object to the processing of personal data, Rakuten will notify other Group Members or any sub-processors to whom the personal data has been disclosed accordingly, who will also update their records.

8.4 If the request made to Rakuten is to object to the processing of that individual's personal data because the rights and freedoms of the individual are prejudiced by virtue of such processing by Rakuten, or on the basis of other compelling legitimate grounds, the matter

will be referred to the Global Privacy Office to assess. Where the processing undertaken by Rakuten is required by law, the request will not be regarded as valid.

9. REQUESTS FOR DATA PORTABILITY

9.1 Under European data protection law individuals have the right to receive their personal data which they have provided to Rakuten in a structured, commonly-used and machine-readable format, and have the right to request that this information be sent by Rakuten to another controller, where technically feasible. This is called the right to data portability under European data protection law.

9.2 The right to data portability only applies:

(a) To personal data an individual has provided to Rakuten (not inferred or derived data that are created by Rakuten as a result of analysis of data provided by the individual (e.g. algorithmic results));

(b) Where the processing of that personal data is based on the individual's consent (e.g. for the processing of special categories of personal data) or is for the performance of a contract; and

(c) When processing is carried out by automated means (i.e. via an IT system, not hard copy / paper records).

9.3 The request shall be answered within one month. This can be extended to two months where the request is complex or where Rakuten receives a number of requests.

9.4 Rakuten will compile the personal data about the requestor that meets the requirements set out in 9.1 and 9.2 above. Rakuten may deny a request for data portability on grounds permitted under European data protection law or applicable local law. This assessment shall be made by the Global Privacy Office.

APPENDIX 2

Privacy Training Requirements

Binding Corporate Rules Policy of Rakuten

Privacy Training Requirements

1. BACKGROUND

1.1 The Binding Corporate Rules Policy of Rakuten (the "**Policy**") provides a framework for the transfer of personal data between Rakuten group members ("**Group Members**"). The purpose of the Privacy Training Requirements document is to provide a summary as to how Rakuten trains its staff (the "**employees**") on the requirements of the Policy.

1.2 Rakuten's Global Privacy Office within the IT Security Governance Department has overall responsibility for privacy compliance training within Rakuten, including the delivery and monitoring of Rakuten's privacy training programs. Training on the Policy is overseen by the Global Privacy Manager and the Global Privacy Office.

1.3 All Rakuten employees receive periodic training on privacy and data protection (the "**General Privacy Training**") and information security.

1.4 Employees who have permanent or regular access to personal data, who are involved in the collection of personal data or in the development of tools to process personal data receive additional, tailored training on the Policy (the "**BCR Policy Training**") and specific data protection issues relevant to their role and location. This training is further described below and is carried out on a regular basis.

1.5 The General Privacy training and the BCR Policy training together are referred to in this document as the "**Privacy and Compliance Training Program**".

2. OVERVIEW OF TRAINING AT RAKUTEN

2.1 All Rakuten employees are required to participate in the General Privacy training program once every [two] years. The program is called the Data Privacy and Security Training program.

2.2 The General Privacy Training covers a range of subjects, including data privacy, data breaches, and Rakuten's Privacy and Information Security policies and procedures.

2.3 In addition to the training described in section 2.1 and 2.1, Rakuten also provides specific training on the Policy as described in section 4 below.

3. AIMS OF THE PRIVACY AND COMPLIANCE TRAINING PROGRAM AT RAKUTEN

3.1 The aim of Rakuten's **Privacy and Compliance Training Program** is to help create and maintain an environment in which employees:

(a) have an understanding of the basic principles of data privacy, confidentiality, and information security;

(b) understand Rakuten's Privacy and Information Security policies and procedures; and

(c) having permanent or regular access to personal data, who are involved in the collection of personal data or in the development of tools to process personal data, receive appropriate training, as described in section 4, to enable them to process personal data in accordance with the Policy.

3.2 General data protection and privacy training for new employees

(a) New employees must complete the General Privacy Training and the BCR Policy Training (if required) shortly after joining Rakuten.

3.3 General data protection and privacy training for all employees

(a) Employees worldwide receive the General Privacy Training. This training covers basic data privacy rights and principles and data security in line with the requirements of the Policy. It is designed to be both informative and user-friendly, generating interest in the topic. Completion of the course is monitored and enforced by Rakuten's Global Privacy Office, which drives 100% completion by all required employees annually and is accountable to the Chief Compliance Officer.

(b) All employees also benefit from ad-hoc communications consisting of emails, awareness messaging placed on Rakuten's intranet pages which convey the importance of information security and data protection issues relevant to Rakuten, including for example, social networking, remote working, engaging data processors and the protection of confidential information.

4. BCR POLICY TRAINING

4.1 Rakuten's training on the Policy will cover the following main areas and employees receive training appropriate to their roles and responsibilities within Rakuten:

(a) Background and rationale:

(i) What is data protection law?

(ii) How data protection law will affect Rakuten internationally

(iii) The scope of the Policy

(iv) Terminology and concepts

(b) The Policy:

(i) An explanation of the Policy

(ii) Practical examples

(iii) The rights that the Policy gives to individuals

(c) Where relevant to an employee's role, training will cover the following procedures under the Policy:

(i) Subject Access Request Procedure

(ii) Audit Protocol

(iii) Updating Procedure

(iv) Cooperation Procedure

(v) Complaint Handling Procedure

5. FURTHER INFORMATION

Any queries about training under the Policy should be addressed to the Global Privacy Office which can be contacted at: rakuten-privacy@mail.rakuten.com.

APPENDIX 3

Audit Protocol

Binding Corporate Rules Policy of Rakuten

Audit Protocol

1. **BACKGROUND**

1.1 The purpose of Rakuten's Binding Corporate Rules Policy (the "**Policy**") is to safeguard personal data transferred between the Rakuten group members ("**Group Members**").

1.2 In the European Member States from which personal data is transferred and where applicable in other countries as required by local data protection laws, the Policy requires approval from the data protection authorities. A requirement of some data protection authorities is that Rakuten audits compliance with the Policy and satisfies certain conditions in so doing. This document describes how Rakuten deals with such requirements.

1.3 The role of Rakuten's Global Privacy Manager in the group headquarters in Japan and the Global Privacy Office is to provide guidance about the collection and use of personal data subject to the Policy and to assess the collection and use of personal data by Group Members for potential privacy-related risks. The collection and use of personal data is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol describes the formal assessment process adopted by Rakuten to ensure compliance with the Policy as required by the data protection authorities, this is only one way in which Rakuten ensures that the provisions of the Policy are observed and corrective actions taken as required.

2. **APPROACH**

2.1 Overview of audit

(a) Compliance with the Policy is overseen on a day to day basis by the Global Privacy Office.

(b) The Internal Audit Department, which includes accredited auditors, will be responsible for performing and/or overseeing independent audits of compliance with the Policy and will ensure that such audits address all aspects of the Policy. The Internal Audit Department will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of the Global Privacy Manager and that any corrective actions to ensure compliance take place within a reasonable timescale.

2.2 Timing and scope of audits

(a) Audits of the Policy will take place:

(i) annually in accordance with Rakuten's audit procedure/s; and

(ii) more frequently at the request of the Global Privacy Manager; and

(iii) if determined necessary by the Global Privacy Manager.

(b) The scope of the audit performed will be determined by the Internal Audit Department on a risk-based analysis which will consider relevant criteria, for example: areas of current regulatory focus, industry specific requirements where applicable, areas of specific or new risk for the business, areas of non-compliance, areas with changes to the systems or processes used to safeguard information,

areas where there have been previous audit findings or complaints, the period since the last review, and the nature, method and location of the personal data processed.

2.3 Auditors

Audit of the procedures and controls in place to give effect to the commitments made in the Policy will be undertaken by Rakuten's Internal Audit Department and Rakuten may use other accredited internal/external auditors as determined by Rakuten.

2.4 Report

On completion of the audit the report and findings will be made available to the Global Privacy Manager and Rakuten, Inc. A summary of the findings will be provided to the Board of Directors with details of any remedial action required, recommendations and timescales for remedial action to be undertaken.

Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Rakuten has agreed to provide copies of the results of any audit of the Policy to data protection authorities of competent jurisdiction.

Rakuten's Global Privacy Manager will be responsible for liaising with the data protection authorities of competent jurisdiction for the purpose of providing the information outlined above.

In addition, Rakuten has agreed that data protection authorities of competent jurisdiction may audit Group Members for the purpose of reviewing compliance with the Policy in accordance with the terms of the Co-operation Procedure which is attached as Appendix 5 of the Binding Corporate Rules Policy of Rakuten.

APPENDIX 4

Complaint Handling Procedure

BINDING CORPORATE RULES POLICY OF RAKUTEN

Complaint Handling Procedure

1. **INTRODUCTION**

1.1 The Binding Corporate Rules Policy (the "**Policy**") safeguards personal data transferred between members of the Rakuten Group ("**Group Members**"). The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose personal data is processed by Rakuten under the Policy are dealt with.

2. **HOW INDIVIDUALS CAN BRING COMPLAINTS**

2.1 All complaints made under the Policy can be brought in writing to Rakuten's Global Privacy Office at Rakuten Europe S.à r.l. at rakuten-privacy@mail.rakuten.com.

3. **WHO HANDLES COMPLAINTS?**

3.1 Rakuten's Global Privacy Office or where appropriate the local privacy contact will handle all complaints arising under the Policy. Rakuten's Global Privacy Office will liaise with the relevant business units to investigate the complaint. The Global Privacy Office will coordinate a response.

4. **WHAT IS THE RESPONSE TIME?**

4.1 Rakuten's Global Privacy Office will acknowledge receipt of a complaint to the individual concerned within 5 working days, and investigate and make a substantive response within two months. If, due to the complexity of the complaint, a substantive response cannot be given within this period, Rakuten's Global Privacy Office will advise the complainant accordingly and provide a reasonable estimate (not exceeding six months) for the timescale within which a response will be provided.

5. **WHEN A COMPLAINANT DISPUTES A FINDING**

5.1 If the complainant disputes the response of the Global Privacy Office (or the individual or department within Rakuten dealing with the complaint) or any aspect of a finding, and notifies Rakuten accordingly, the matter will be referred to the Chief Compliance Officer who will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Chief Compliance Officer will respond to the complainant within six months of the referral. If the complaint is upheld, the Chief Compliance Officer will arrange for any necessary steps to be taken as a consequence.

Rakuten acknowledges that some data protection laws provide individuals with the right to make a complaint to a data protection authority or other competent authority and/or lodge claims with a court of competent jurisdiction regardless of whether they have first made a complaint to Rakuten (such as the data protection laws in Europe as reflected in Section C).

APPENDIX 5

Co-operation Procedure

BINDING CORPORATE RULES POLICY OF RAKUTEN

Co-operation Procedure

1. **INTRODUCTION**

This Co-operation Procedure sets out the way in which Rakuten will co-operate with the data protection authorities with competent jurisdiction over the Binding Corporate Rules Policy (the "**Policy**").

2. **CO-OPERATION PROCEDURE**

2.1 Where required, Rakuten will make the necessary personnel available for dialogue with a data protection authority with competent jurisdiction over the Policy.

2.2 Rakuten will actively review and consider:

(a) any decisions made by relevant data protection authorities on any data protection law issues that may affect any aspect of the processing of personal data referred to in the Policy; and

(b) where applicable, the views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules.

2.3 Subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Rakuten will provide upon request copies of the results of any audit of the Policy to a data protection authority with competent jurisdiction.

2.4 Rakuten agrees that:

(a) where any Rakuten group member ("**Group Member**") is located within the jurisdiction of a data protection authority based in Europe, Rakuten agrees that that particular data protection authority may audit that Group Member for the purpose of reviewing compliance with the Policy, in accordance with the applicable law of the country in which the Group Member is located; and

(b) in the case of a Group Member located outside Europe, Rakuten agrees that a data protection authority with competent jurisdiction may audit that Group Member for the purpose of reviewing compliance with the Policy in accordance with the applicable law of the country from which the personal data is transferred under the Policy, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Rakuten (unless this requirement is in conflict with local applicable law).

2.5 Rakuten agrees to abide by a formal decision of the applicable data protection authority where a right to appeal is not exercised on any issues relating to the interpretation and application of the Policy, or any aspect of it.

APPENDIX 6

Updating Procedure

BINDING CORPORATE RULES POLICY OF RAKUTEN

Updating Procedure

1. **INTRODUCTION**

This Binding Corporate Rules Updating Procedure sets out the way in which Rakuten will communicate changes to the Binding Corporate Rules Policy (the "**Policy**") to the data protection authorities with jurisdiction over the Policy, data subjects, its customers, merchants and to the Rakuten group members ("**Group Members**") bound by the Policy.

2. **MATERIAL CHANGES TO THE POLICY**

2.1 Rakuten will communicate any material changes to the Policy as soon as is reasonably practical to the National Commission for Data Protection in Luxemburg ("**CNPD**") and to any other relevant data protection authorities with jurisdiction over the Policy in accordance with their requirements.

3. **ADMINISTRATIVE CHANGES TO THE POLICY**

3.1 Rakuten will communicate changes to the Policy which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of applicable data protection law in any relevant country, through any legislative, court or supervisory authority measure to the CNPD and to any other data protection authorities with jurisdiction over the Policy at least once a year. Rakuten will also provide a brief explanation to the CNPD and to any other relevant data protection authorities of the reasons for any notified changes to the Policy.

4. **COMMUNICATING AND LOGGING CHANGES TO THE POLICY**

4.1 The Policy contains a change log which sets out the date of revisions to the Policy and the details of any revisions made. Rakuten's Global Privacy Manager will maintain an up-to-date list of the changes made to the Policy.

4.2 Rakuten will communicate all changes to the Policy, whether administrative or material in nature:

(a) to the Group Members bound by the Policy; and

(b) to the data subjects who benefit from the Policy via public notifications published appropriately.

4.3 Rakuten's Global Privacy Manager will maintain an up-to-date list of the Group Members bound by the Policy. This information will be made available by Rakuten upon request.

5. **NEW GROUP MEMBERS**

Rakuten's Global Privacy Manager will ensure that all new Group Members are bound by the Policy before a transfer of personal data to them takes place.