Effective date: April 2025

Ef þú vilt óska eftir upplýsingum um innihald Skuldbindandi reglna fyrirtækja American Express hjá ESB á staðbundið tungumáli þínu, vinsamlegast sendu tölvupóst á dpo-europe@aexp.com og tilgreindu viðeigandi staðbundið tungumál Beiðnir verða afgreiddar innan sanngjarnra tímamarka og í samræmi við gildi persónuverndarlög

American Express EU Binding Corporate Rules (EU BCRs)

Table of Contents

1. INTRODUCTION

1.1. Overview

American Express values your trust and respects your privacy.

Data protection and information security are long-standing priorities for our company. As a multinational organization, We are committed to protecting personal data, irrespective of where it is used, and all personal data American Express collects is handled according to our Data Protection and Privacy Principles.

In 2012, American Express was one of the first companies to publish Binding Corporate Rules (BCRs) approved by the Information Commissioner's Office. Today, these BCRs continue to lay a framework for our strong privacy commitments, promoting a robust compliance culture across our enterprise.

Amongst other things, our BCRs govern the international Transfers of Personal Data within the American Express BCRs Entities in accordance with Applicable Data Protection Legislation and ensure that your Personal Data is always adequately protected regardless of where it is Transferred.

1.2. Easy access to the BCRs

Our BCRs are available for You to access on American Express' websites across Europe. You may also request a copy of our BCRs in an alternative format from our Data Protection Officer ("DPO") at the address below or from the American Express BCRs Entity responsible for your Personal Data. Please note that the lead Supervisory Authority overseeing our BCRs is the Agencia Española de Protección de Datos (AEPD) ("Lead Supervisory Authority").

2. BINDING NATURE OF THE BCRs

Our BCRs are legally binding on the American Express BCRs Entities and their Employees by an Intra-Group Agreement between American Express Company and AEESA, the legal representative of American Express in the EEA. AEESA is the European company within American Express that has assumed responsibility for ensuring that Personal Data is Processed in accordance with the BCRs.

Each American Express BCRs Entity and their Employees may only Process Personal Data under the scope of these BCRs in accordance with these BCRs. Employees who violate these BCRs may be subject to disciplinary actions.

3. SCOPE OF OUR BCRs

3.1. Geographical scope

Our BCRs apply to all Processing by American Express BCRs Entities of Personal Data subject to Applicable Data Protection Legislation, as follows:

(a) to Personal Data of a Data Subject Transferred by an American Express BCRs Entity to an American Express BCRs Entity located in a Third Country; and

(b) to Personal Data of a Data Subject that is onward Transferred to other American Express BCRs Entities located in a Third Country.

The American Express group is structured through different legal entities around the world. The parent company of the group is the legal entity American Express Company. AEESA and the other American Express BCRs Entities are either directly or indirectly owned by American Express Company.

A list of the American Express BCRs Entities is set out in Appendix 2.

3.2. Material scope

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

In its capacity as Data Controller, American Express Processes the Personal Data of past, present and prospective employees, directors, contractors, individual consultants, contingent workers, employed by American Express whether full time, part time, permanent or temporary, as well as retirees ("Employees") and the Personal Data of past, present and prospective American Express consumers, and natural persons working at the corporate clients, suppliers and partners of American Express ("Customers").

The purposes for which American Express Processes Personal Data mainly relate to consumer, commercial, merchant, insurance, travel, meetings and events, and network services as well as human resources.

To effectively conduct American Express' global activities, the Processing of Personal Data by the American Express BCRs Entities, in connection with the purposes identified in these BCRs, may involve international Transfers of Personal Data of Data Subjects, from any American Express BCRs Entity subject to the GDPR to any other American Express BCRs Entity in a Third Country (including from countries in the EEA to the United States, where American Express' main servers are located), and any other onward Transfer to American Express BCRs Entities in a Third Country.

For a more comprehensive view of American Express' Processing activities, please refer to Appendix 1. To see where our American Express BCRs Entities are located, please refer to Appendix 2.

4. HOW DOES AMERICAN EXPRESS PROTECT YOUR PERSONAL DATA?

When Processing your Personal Data, American Express BCRs Entities are committed to complying with robust data protection principles (section 4.1) and to respecting your data protection rights (section 4.2).

4.1.Data protection principles

4.1.1. Transparency and fairness

The American Express BCRs Entities will collect and Process your Personal Data in a transparent manner and by fair means.

We ensure that You are provided with easy access to the information on our Processing activities as required by the GDPR. This information is provided to You in a concise, transparent, intelligible and easily accessible form, using clear and plain language and is available in the relevant American Express Privacy Statements, as applicable to your relationship with Us. These notices and terms and conditions may also contain additional provisions which are relevant to the Processing of Personal Data, pursuant to national/local applicable law(s) and regulation(s) of the relevant American Express BCRs Entity.

In particular, when the Personal Data is collected from the Data Subject, the following information will be provided at the moment the Personal Data is collected:

- the identity and contact details of the Controller and, where applicable, its representative;

- the contact details of the DPO;

- the purposes of the Processing for which the Personal Data are intended and the legal basis for the Processing including an explanation about the legitimate interests pursued, where applicable;

- the recipients or categories of recipients of the Personal Data, if any;

- the existence of Personal Data Transfers and information about the appropriate safeguards adopted to ensure the same level of protection as required by the GDPR and how to access or obtain a copy of such safeguards. In the case of Transfers of Personal Data between a Data Exporter and a Data Importer based on these BCRs, the information provided will include reference to these BCRs and how to access them;

- the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

- the existence of the Data Subjects' rights recognised by the GDPR and how to exercise such rights;

- whether the provision of the information is a statutory or contractual requirement, and the consequences of the failure to provide Personal Data in such circumstances; and

- information about the existence of automated decision-making, including profiling, and at least in cases where such decisions produce legal effects concerning the Data Subjects or similarly significantly affect the Data Subjects, or are based on Special Categories of Data, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subjects.

When the Personal Data has not been collected from the Data Subject, the previous information, as well as the categories of Personal Data concerned and the source from which the Personal Data originates, will be communicated in a timely manner and in accordance with the timescales required under Applicable Data Protection Legislation (unless the Data Subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort, obtaining or disclosure is expressly laid down by Union or Member State law or where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy).

Our BCRs also: (a) inform You about the rights You are entitled to enforce against AEESA or any American Express BCRs Entity as third-party beneficiary with regard to the Processing of your Personal Data under these BCRs ("Third-party Beneficiary Rights") and on the means to exercise such rights (see section 8); (b) provide You with a description of the scope of the BCRs; (c) provide You with information on the data protection principles that We apply

when Processing your Personal Data (as explained in this section 4); and (c) provide You with information about the liability American Express BCRs Entities assume in the event of a breach of these BCRs (see section 8).

In addition, You are always able to obtain, upon request, a copy of our BCRs. Our BCRs are available on American Express BCRs Entities' public websites across the EEA as well as on our intranet if You are an Employee.

4.1.2. Lawfulness of Processing

Your Personal Data and Special Categories of Data are collected and Processed fairly and lawfully, in accordance with the Applicable Data Protection Legislation. The lawful bases for Processing your Personal Data are described in more detail in the relevant American Express Privacy Statements, as applicable to your relationship with American Express.

• Processing of Personal Data

Your Personal Data is collected and Processed only where there is a lawful basis for Processing, including:

- when You have given your Consent to the Processing of your Personal Data (for instance, to send You email communications containing ads, promotions, and offers for American Express products and services);

- when the Processing is necessary for the performance of a contract to which You are a party or in order to take steps at your request prior to entering into a contract (for instance, to administer our contractual relationship with You and process your application for a card, account or other product or to manage your existing accounts);

- when the Processing is necessary for compliance with a legal obligation (for instance, to report certain suspicious transactions to the competent authorities under anti-money-laundering rules or as required by law to perform due diligence on Customers before approving their applications);

- when the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person (for instance, if We need to Process Employee data for the purpose of emergency medical care);

- when 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 the Data

Controller (for instance, for tax purposes, where laid down by Member State law to which the relevant Data Controller is subject); or

- when the Processing is necessary for the purposes of the legitimate interests pursued by an American Express BCRs Entity or by third-party(ies) (for instance, to deliver products and services, advertise and market products and services, conduct research and analysis, and manage our fraud and security risks. An example of us managing fraud and security risks could be where one entity shares information with another that it deems to be suspicious to enable us to contact the Customer to review it), except where such interests are overridden by your interests or fundamental rights and freedoms.

• Processing of Special Categories of Data

We may collect Special Categories of Data.

This data is collected and Processed only where necessary for the purpose of Processing. To the limited extent that Special Categories of Data are collected, they will only be Processed under one of the lawful basis mentioned above, and provided one of the conditions for Processing Special Categories of Data applies, as follows:

- You have given your explicit Consent to the Processing of your Personal Data for one or more specified purposes, except where Applicable Data Protection Legislation provides that the prohibition to processing Special Categories of Data may not be lifted by the Data Subject;

- the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

- the Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;

- the Processing relates to Special Categories of Data which You have manifestly made public;

- the Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

- the Processing is necessary for reasons of substantial public interest, on the basis of Applicable Data Protection Legislation, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

- the Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Applicable Data Protection Legislation or pursuant to contract with a health professional and provided that the Processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under Applicable Data Protection Legislation or by rules established by national competent bodies;

- the Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Applicable Data Protection Legislation which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

- the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Applicable Data Protection Legislation which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

- if You are an Employee and the Processing is necessary for the purpose of carrying out the obligations and specific rights of American Express or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Applicable Data Protection Legislation or a collective agreement pursuant to Applicable Data Protection Legislation, providing for appropriate safeguards for the fundamental rights and interests of Data Subjects;

Where the Processing of Personal Data relates to criminal convictions and offences or related security measures, American Express BCRs Entities will not carry out such Processing other than under the control of official authority or when the Processing is authorised by law providing appropriate safeguards for the rights and freedoms of Data Subjects in accordance with the lawful bases above.

In addition, given the higher level of protection Special Categories of Data receive under Applicable Data Protection Legislation, the American Express BCRs Entities will take reinforced measures to Process Special Categories of Data, as required by the Applicable Data Protection Legislation.

4.1.3. Data minimization, accuracy and storage limitation

The American Express BCRs Entities use appropriate technology and established Employee practices to Process your Personal Data promptly and accurately.

We take reasonable steps to ensure that your Personal Data is:

- Accurate and, where necessary, kept up to date having regard to the purposes for which it is Processed (data accuracy). Inaccurate Personal Data is erased or rectified without delay. We have adopted measures to ensure that incorrect Personal Data is erased, corrected, supplemented or rectified (as necessary). For example, Our Data Processors are contractually obliged to cooperate and assist Us with fulfilling this requirement under Applicable Data Protection Legislation. We also have policies in place which set out standards that American Express BCRs Entities must adhere to;

- Adequate, relevant and not excessive in relation to the purpose for which the Personal Data is collected and Processed (data minimization). In particular, We take this into account in our initial collection of data from Data Subjects (for example, in our application form for cardmembers), to ensure We only collect the minimum amount of Personal Data necessary to fulfil the relevant purpose;

- Not kept in an identifiable form for longer than necessary for the purposes for which the Personal Data is Processed, and only retained for a longer period for archival purposes or as otherwise permitted or required to be retained in accordance with applicable law(s) (for example, the local law of the relevant American Express BCRs Entity located in a Third Country), and then only when appropriate administrative, technical and organisational measures are taken. We have implemented a records retention framework within American Express

which sets out appropriate timescales for data records and its retention, and policies which set out standards that American Express BCRs Entities must adhere to.

4.1.4. Purpose limitation

The American Express BCRs Entities only collect Personal Data for specific and legitimate purposes. We Process your Personal Data fairly and only for those purposes We have told You, for purposes permitted by You or by the Applicable Data Protection Legislation. One of the ways in which We ensure compliance with this principle is by embedding privacy and data protection standards into our new product approval process.

We will ensure that your Personal Data is not further Processed in a manner that is incompatible with such purposes.

4.1.5. Data security and confidentiality

American Express operates within a heavily regulated environment and its regulators hold American Express to consistently high and stringent standards with respect to its information security and privacy practices. American Express has implemented and commits to maintain a comprehensive written information security program that complies with applicable law(s) (including those that may be applicable to an American Express BCRs Entity located in a Third Country) and Applicable Data Protection Legislation.

The American Express BCRs Entities implement appropriate administrative, technical and organizational measures to protect your Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data transmitted, stored or otherwise Processed. We will keep your Personal Data confidential and limit access to your Personal Data to those who specifically need it to conduct their business activities, except as otherwise required by law applicable to Us.

Such measures ensure a level of security appropriate to the risk and take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, and may include as appropriate:

- the pseudonymisation and encryption of Personal Data (such as, where appropriate, tokenisation and access management controls),

- measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (for example, cryptographic standards and policies to support and govern our processes);

- measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

We also require appropriate administrative, technical and organisational measures from those third-parties who are authorised by Us to Process your Personal Data on our behalf (and may include the above measures, as appropriate) and We enter into contractual commitments with internal and external Data Processors that comply with safeguards required by the GDPR.

In particular, Processing by the Data Processor (including internal Data Processors within the American Express group and external Data Processors) shall be governed by a contract, that is binding on the Data Processor with regard to the Data Controller and that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Data Controller.

The following duties must also be covered in the agreement that must require the Data Processor to:

- Process the Personal Data only on documented instructions from the Data Controller, including with regard to Transfers of Personal Data, unless required to do so by a law to which the Data Processor is subject (in such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest);

- ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- take all appropriate technical and organizational measures required to guarantee an acceptable level of security appropriate to the risk involved in the Processing of the Personal Data;

- not contract another Data Processor ("Sub-processor"), without prior specific or general written authorisation of the Data Controller and only provided that the same data protection obligations as set out in the contract between the Data Controller and the Data Processor are imposed on that Sub-processor (in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Applicable Data Protection Legislation);

- taking into account the nature of the Processing, assist the Data Controller with appropriate technical and organizational measures whenever possible for the fulfilment of the duty of the Data Controller to respond to any requests from Data Subjects exercising their rights;

- assist the Data Controller with the fulfilment of its obligations regarding security of Processing, Personal Data Breaches and Data Protection Impact Assessments (including if consultation with a Competent Supervisory Authority is required in relation to a Data Protection Impact Assessment);

- at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to Processing, and delete existing copies unless the applicable law (for example, the local law of the relevant American Express BCRs Entity located outside of the EEA) requires storage of the Personal Data;

- make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller; and

- immediately inform the Data Controller if, in the Data Processor's opinion, an instruction from the Data Controller infringes Applicable Data Protection Legislation.

In addition, the American Express BCRs Entities have implemented administrative, technical and organisational measures to detect, investigate, escalate and remediate Personal Data Breaches.

AEESA and the American Express DPO are notified of Personal Data Breaches by the relevant American Express BCRs Entity without undue delay. If an American Express BCRs Entity is acting as a Data Processor on behalf of another American Express BCRs Entity (as the Data Controller), the Data Processor shall notify that Data Controller without undue delay.

The American Express DPO shall determine whether to notify: (a), the Competent Supervisory Authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the Personal Data Breach (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subjects); and (b) any Data Subjects where the breach is likely to result in a high risk to their rights and freedoms, in both cases in accordance with GDPR requirements.

Any Personal Data Breaches are documented (comprising the facts relating to the Personal Data Breach, its effects, and the remedial action taken) and the documentation is made available to the Competent Supervisory Authority on request.

4.1.6. Onward Transfers

Your Personal Data is Transferred throughout American Express BCRs Entities and onward to third-parties, always ensuring an adequate level of protection for the Processing of your data as required by Applicable Data Protection Legislation, regardless of where it is Transferred.

This flow of data is legitimized through our BCRs, which allow Us to Transfer Personal Data from the EEA to the American Express BCRs Entities located in Third Countries .

In all cases of onward Transfers (i.e., Personal Data that has first been Transferred from an American Express BCRs Entity to a non-EEA American Express BCRs Entity and later transferred to third-party(ies) not covered by the BCRs), the American Express BCRs Entities will ensure that:

(a) they enter into a written agreement with these third-parties containing provisions that ensure the Personal Data is protected at least to the confidentiality and security standard contemplated by these BCRs (and where such third-party is a Data Processor, the Data Processor duties set out in section 4.1.5 of these BCRs will also be included in such written agreement); and

(b) in the absence of an adequacy decision, use an appropriate safeguard to ensure that the Transfer is lawful and adequate guarantees are given under Article 46 of the GDPR.

In the absence of an adequacy decision or appropriate safeguards, onward Transfers may exceptionally take place only if a derogation applies in line with Article 49 of the GDPR (for example, if the Transfer is necessary for important reasons of public interest).

4.1.7. Accountability

Each American Express BCRs Entity acting as a Data Controller will be responsible for, and must demonstrate compliance with, these BCRs. Compliance with these requirements includes:

- the maintenance of electronic records of Processing activities carried out on Personal Data Transferred under these BCRs, and available to the Competent Supervisory Authorities on request. These records contain the information required by the GDPR, such as: the name and contact details of the Data Controller and its representative and DPO (where applicable), the purposes of Processing, the categories of Data Subjects and categories of Personal Data, the recipients of the Personal Data, the Transfers to countries outside of the EEA together with the documentation of suitable safeguards implemented to legitimize such Transfers, the time limits for erasure of the categories of Personal Data (where possible) and the description of the security measures applied (where possible).

Each American Express BCRs Entity acting as a Data Processor on behalf of another American Express BCRs Entity shall also maintain an electronic record of Processing activities carried out on Personal Data Transferred under these BCRs on behalf of the relevant Data Controller. These records shall include the following information: the name and contact details of the Data Processor and of the relevant Data Controller and where applicable, of the representative and DPO of both the Data Processor and Data Controller, the categories of Processing carried out on behalf of the Data Controller, Transfers to countries outside of the EEA together with the documentation of suitable safeguards implemented to legitimize such Transfers and the description of the security measures applied (where possible);

- the completion of Data Protection Impact Assessments (applicable only when the Processing activities are likely to result in a high risk to the rights and freedoms of the Data Subjects); and

- where a DPIA indicates that the Processing activities would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk, the relevant American Express BCRs Entity acting as a Data Controller should, prior to Processing, consult with the Competent Supervisory Authority.

In addition, the American Express BCRs Entities have put in place appropriate administrative, technical and organisational measures designed to implement data protection principles and to facilitate compliance with the requirements set up by these BCRs (data protection by design and by default) and to ensure the processing activities carried out by the American Express BCRs Entities are appropriately documented (including via the new product approval process and via the third party lifecycle management programme).

4.2. Data Subjects' rights

• Rights of information, access, restriction, objection, rectification, erasure, right to withdraw Consent and to data portability

The American Express BCRs Entities comply with your requests to exercise the rights entitled to You by the GDPR, where applicable. More specifically, We ensure that You can exercise your right to:

- information (the American Express Privacy Statement that applies to the Processing We undertake in the context of your relationship with Us sets out this information);

- access your Personal Data (right of access). This enables You to receive a copy of the Personal Data We hold about You and to check We are lawfully Processing it;

- restrict the Processing of your Personal Data (right to restriction of Processing). You can ask Us to restrict the processing of your Personal Data in the following scenarios:

  - if You want Us to establish the accuracy of the Personal Data;
  - where our use of the Personal Data is unlawful, but You do not want Us to erase it;

- where You need Us to hold the Personal Data even if We no longer require it as You need it to establish, exercise or defend legal claims; or
- You have objected to our use of your Personal Data but We need to verify whether We have overriding legitimate grounds to use it;

- object to the Processing of your Personal Data (right to object), on the following grounds:
  - on grounds relating to your particular situation when the applicable legal basis is legitimate interests. In some cases, We may demonstrate that We have compelling legitimate grounds to process your Personal Data, which override your rights and freedoms. If this is the case, We will let You know; and
  - when your Personal Data is processed for direct marketing purposes;

- rectify your Personal Data (right to rectification). This enables You to have any incomplete or inaccurate data We hold about You corrected, although We may need to verify the accuracy of the new data You provide to Us;

- erase your Personal Data (right to erasure or right to be forgotten). This enables You to ask Us to delete or remove Personal Data where there is no good reason for Us continuing to process it. You also have the right to ask Us to delete or remove your Personal Data where You have successfully exercised your right to object to Processing (see below), where We may have Processed your information unlawfully or where We are required to erase your Personal Data to comply with applicable law (for example, the local law of the relevant American Express BCRs Entity located outside of the EEA). However, please note that We may not always be able to comply with your request for specific reasons set out in the law which will be notified to You, if applicable, at the time of your request;

- withdraw a previously provided Consent for Processing. This will not affect the lawfulness of any processing carried out before You withdraw your consent. If You withdraw your consent, We may not be able to provide certain products or services to You. We will advise You if this is the case at the time You withdraw your consent; and

- receive your Personal Data in a structured, commonly used and machine-readable format and/or transmit such data to another Data Controller (right to data portability). We will provide to You, or (where technically feasible) a third party you have chosen, your Personal Data in a structured, commonly

used and machine-readable format. Note that this right only applies to automated information for which You initially provided consent for Us to use or where We used the information to perform a contract with You.

We will also notify recipients to whom your Personal Data has been disclosed (unless this provides impossible or involves disproportionate effort) regarding the exercise of your rights with respect to rectification or erasure or restriction of your Personal Data. If You request Us to do so, We will inform You about these recipients.

The American Express BCRs Entities are subject to policies on how to handle such requests to ensure that You have the means to exercise these rights. If You would like to exercise any of your rights, You may contact our DPO at DPO-Europe@aexp.com.

• Automated decision making

The American Express BCRs Entities ensure that You are not subject to decisions based solely on automated Processing of Personal Data, including Profiling, which produce legal effects or similar significant effects, unless the Processing is:

- necessary for entering into or performing a contract between You and American Express;

- authorized by a law to which American Express is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or

- based on your explicit Consent to such Processing.

Where the Processing is based on Consent or is necessary for entering into or performing a contract between You and American Express, We will implement suitable measures to safeguard your rights and freedoms and legitimate interests, which shall at least include the right to obtain human intervention, to express your point of view and to contest the decision.

In compliance with these restrictions, We may use automated processes to help Us make certain decisions, for example, to detect and manage fraud (e.g., to help decide whether your account is used for fraud or money laundering purposes or to detect if fraudsters have accessed your account); or to process card applications and assess credit and security risks. These methods are regularly tested to ensure that they remain fair, effective and unbiased.

You may contact our DPO at DPO-Europe@aexp.com to exercise your right to request a manual review of certain automated Processing activities that may impact your legal or other contractual rights or that may have a similar legal effect.

5. AMERICAN EXPRESS DPO NETWORK

American Express has appointed a DPO who monitors compliance with the BCRs and enjoys the highest management support for fulfilling this task. The DPO, appointed on the basis on professional qualities, reports to the American Express Chief Privacy Officer and has access to the American Express Company's Board via the Chief Privacy Officer's direct line of reporting.

The DPO has the following tasks:

- informs and advises American Express entities and American Express Employees of their obligations under Applicable Data Protection Legislation;

- monitors compliance with Applicable Data Protection Legislation (including training and compliance at a local level) through the assessment of key risk indicators and controls. The DPO reports the results of these monitoring activities to the relevant internal senior-level governance forum;

- provides advice in connection with Data Protection Impact Assessments and monitors their performance;

- reports on privacy-related matters, risks and results to the Board of AEESA and subordinate risk committees, as appropriate;

- advises on new privacy-related laws and regulations and the impact on existing processes;

- advises on compliance with these BCRs;

- cooperates with Supervisory Authorities; and

- acts as a point of contact for Supervisory Authorities (including, for example, in the event of any notifiable personal data breach).

The appointment is communicated to the Supervisory Authorities of the European countries where American Express is established.

The DPO works closely with and is supported by a network of privacy specialists and compliance lawyers located in each European market who monitor compliance with Applicable Data Protection Laws in their region and report major privacy issues to the DPO. The DPO is supported in his/her tasks by the Global Privacy Office led by the American Express Chief Privacy Officer. A summary of the role and tasks of the privacy network are as follows:

- The Global Privacy Office ("GPO") reports to the American Express Chief Privacy Officer. The GPO responsibilities include global privacy risk oversight functions across the enterprise and management of the overall American Express Privacy Program framework.
- Compliance Privacy Subject Matter Experts (individually or as a group) serve as local subject matter expert in the privacy area of compliance for local legal entities.
- American Express' privacy lawyers provide data protection interpretation and guidance on legal requirements to privacy risk stakeholders.
- The 1st line Privacy Practice Centre of Excellence is responsible for supporting business units implementing privacy controls, policies, standards and requirements.
- The Information Security Office is responsible for informing the EU DPO and GPO of any information and cyber security risks.

The DPO is supported in his/her tasks by the Global Privacy Office led by the American Express Chief Privacy Officer. The DPO may be directly contacted using the contact details set out in section 9.

6. TRAINING AND AWARENESS

All American Express BCRs Entities provide appropriate and up-to-date training materials and courses for all Employees, and in particular for Employees who collect, Process, have permanent or regular access to Personal Data or who are involved in the development of tools used to Process Personal Data to ensure that they are aware of their obligations under Applicable Data Protection Legislation and these BCRs (such training covers, among other elements, procedures of managing requests for access to Personal Data by public authorities).

Such courses are mandatory, and their completion is monitored. The training intervals for such courses vary depending on the Employee's role, function and access to Personal Data.

American Express also provides an annual mandatory data protection course to all Employees, and the completion of this course is also monitored.

7. CONTROL AND AUDIT

American Express has implemented a compliance programme that provides for regular compliance checks and audits of American Express BCRs Entities' operations (by internal or, where needed, by external auditors) to ensure that the BCRs and all related policies and procedures are respected and up to date, and where there are indications of non-compliance, to audit and verify compliance with the BCRs.

Data protection audits cover all aspects of the BCRs (e.g., applications, IT systems, onward transfers, etc.), including methods of ensuring that corrective measures and action plans will take place and (where required) have been implemented.

The audit frequency is determined on the basis of the risk(s) posed by the Processing activities covered by these BCRs to the rights and freedoms of Data Subjects. Regular audits are undertaken every two years, taking a risk-based approach.

Additional data protection audits may be requested by the DPO upon his/her own initiative, at the request of American Express' network of relevant privacy specialists or upon specific request of an American Express BCRs Entity. American Express' internal audit group, as an independent control body, will assess the opportunity and feasibility of these audit requests according to their risk assessment framework.

The audit plan and programme and the entity responsible for performing audits of compliance with the BCRs will be determined by the department within American Express that has requested the audit. The independence of the relevant departments (and those in charge of carrying out the audit) is guaranteed in respect of any request to carry out an audit and the performance of their duties relating to such audit.

If audits are carried out by external auditors, the following conditions under which such auditors are entrusted shall apply:

- the external auditor should be independent, appropriately qualified, have appropriate security clearance and not be a competitor of American Express or its suppliers.
- the scope, term and duration of the audit shall be mutually agreed upon with the external auditor prior to such audit taking place.
- the external auditor will be subject to appropriate confidentiality obligations pursuant to a written agreement in place with such auditor.

The results of these compliance checks and audits will be communicated to the Global Privacy Office of American Express, the DPO, the Board of AEESA, the Competent Supervisory Authorities (if requested by a Competent Supervisory Authority) and where appropriate, made available to the Audit Committee of the Board of Directors of American Express Company.

Where a compliance gap is found, the relevant American Express BCRs Entity must follow any specific guidance from the DPO to ensure verification of compliance with the BCRs. Where the relevant American Express BCRs Entity cannot comply with the specific guidance as a result of local laws and practices, the process set out in section 11.1 of these BCRs shall be followed.

American Express will also co-operate with any compliance checks conducted by any Supervisory Authority with applicable jurisdiction, whether commenced in response to a complaint from a Data Subject, or by the Supervisory Authority's own initiative .

8. COMPLIANCE, ENFORCEMENT AND LIABILITY

8.1. Liability of American Express BCRs Entities

Each American Express BCRs Entity is responsible for complying with the BCRs. In addition to the individual responsibilities of the American Express BCRs Entities, AEESA will accept responsibility for any breach of the BCRs by an American Express BCRs Entity located in a Third Country. AEESA agrees to and shall be entitled to take any necessary action to remedy the acts or omissions of such American Express BCRs Entity that Process Personal Data in violation of the BCRs.

AEESA is liable to pay compensation due for any material or non-material damages suffered by Data Subjects arising in connection with any breach of the BCRs by an American Express BCRs Entity located in a Third Country. All compensation paid will be in full satisfaction of the Data Subject's claim against all American Express BCRs

Entities. For the avoidance of doubt, AEESA's liability extends to the acts or omissions of any American Express BCRs Entity that is situated in a Third Country that breaches the BCRs.

If an American Express BCRs Entity (including when that entity is situated in a Third Country) violates the BCRs, the competent European courts will have jurisdiction in relation to such violation. To the extent that an American Express BCRs Entity located in a Third Country breaches the BCRs, Data Subjects, Supervisory Authorities and courts of applicable jurisdictions may exercise their rights and bring a claim against AEESA as if such conduct had been performed by AEESA in the Member State in which it is based (for more information about how to lodge a complaint, please refer to section 9 below). To the extent that an American Express BCRs Entity located in the EEA breaches the BCRs, Data Subjects may exercise their rights under these BCRS against that American Express BCRs Entity (for more information about how to lodge a complaint, please refer to section 9 below).

8.2. Third-Party Beneficiary Rights

Each Data Subject may enforce against AEESA or any American Express BCRs Entity, the terms of the following provisions of the BCRs as a third-party beneficiary:

- data protection principles (Section 4.1.1 – 4.1.6, inclusive);

- easy access to BCRs (Section 1.2);

- Data Subjects' rights (Section 4.2);

- jurisdiction and liability (Section 8.1);

- this third-party beneficiary clause itself (Section 8.2);

- right to complain through the American Express internal complaint mechanism (Section 9);

- the right to judicial remedies and the right to seek redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCRs as set out under this Section 8.2 as well as the right to lodge a complaint with the Supervisory Authority and before the competent European court (judicial remedies, redress and compensation) (Section 9);

- co-operation with Supervisory Authorities (Section 10);

- conflict of laws affecting compliance with the BCRs and government access requests (Section 11); and

- duty to inform Data Subjects about any updates of the BCR-C and of the list of BCR members (Section 14).

These rights do not extend to those elements of the BCRs pertaining to internal mechanisms implemented within American Express BCRs Entities, such as details of training, audit programme, compliance network, and mechanism for updating the same.

8.3. Burden of proof

Where a Data Subject can demonstrate that they have suffered damage and establish facts which show that it is likely that the damage occurred because of a breach of the BCRs, AEESA bears the burden of proof in demonstrating that the American Express BCRs Entity situated in a Third Country is not liable for any purported breach of the BCRs that gives rise to the Data Subject's claim for compensation for damages, or that no such breach took place.

Where AEESA can prove that an American Express BCRs Entity located in a Third Country is not responsible for the event giving rise to the damage, AEESA and such company may discharge itself from such responsibility and liability.

9. HOW CAN YOU LODGE A COMPLAINT AND ENFORCE THE EU BCRs?

If You want to submit a complaint or claim and exercise your rights in relation to these BCRs (including in relation to any American Express BCRs Entity), You are encouraged to contact the DPO at any time in the following ways: (a) in writing at AEESA's headquarters at American Express Europe SA, Avenida Partenón 12 – 14, 28042 Madrid / SPAIN; or (b) via email at DPO-Europe@aexp.com. While We would encourage You to use one of the contact methods listed above, it is not mandatory for You do so.

Our complaint management team will address your complaints in writing without undue delay and in any event, within one month. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by an additional two months, in which case We will inform You in writing accordingly.

Note that:

- If your complaint is upheld, the relevant American Express BCRs Entity will take appropriate remedial measures to resolve your complaint and ensure compliance with the BCRs, as appropriate;

- If your complaint is rejected, We will explain the reasons for doing so/ the matter will be referred to the DPO 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 within one (1) calendar month; and

- If your complaint is delayed without reason, You should notify the DPO who will, without undue delay and in any event within ten (10) working days, explain the reasons for such delay and explain the actions taken so far.

In addition to our complaints process set out above, Data Subjects can seek redress via the following methods (including if your complaint is not resolved to your satisfaction). Please note that the below rights may be exercised regardless of whether or not You have followed our complaints process beforehand:

- lodge a complaint with the Supervisory Authority in the Member State of your habitual residence, place of work or place of the alleged infringement;

- bring your claim before a competent court of the Member State where the relevant American Express BCRs Entity is established or where You have your habitual residence, and where appropriate, obtain compensation for the damages You suffered as a result of the breach of the above-mentioned Third-Party Beneficiary Rights.

All American Express BCRs Entities accept that Data Subjects may be represented by a not-for-profit body, organisation or association under the conditions set under Article 80(1) of the GDPR.

10. DUTY OF COOPERATION WITH SUPERVISORY AUTHORITIES

All American Express BCRs Entities will:

- co-operate with, and accept to be audited and inspected (including where necessary, on-site) by, any Competent Supervisory Authority on any issues regarding these BCRs;

- take into account the advice of these Supervisory Authorities on any issues regarding these BCRs; and

- abide by decisions of any Competent Supervisory Authority, subject to the right to challenge or appeal such findings or decision, on any issue relating to these BCRs.

All American Express BCRs Entities shall, upon request, provide the Competent Supervisory Authorities with any information about the Processing activities covered by these BCRs.

Any dispute relating to the Competent Supervisory Authority's exercise of its powers to supervise compliance with the BCRs will be resolved by the courts of that Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The relevant American Express BCRs Entities shall submit themselves to the jurisdiction of those courts.

11. HOW DO WE HANDLE POTENTIAL CONFLICTS OF LAWS AND DEAL WITH GOVERNMENT ACCESS REQUESTS?

11.1. Local laws and practices affecting compliance with the EU BCRs

Each American Express BCRs Entity will only use the BCRs as a tool for Transfers where it has been assessed that the law and practices in the Third Country applicable to the Processing of the Personal Data by the relevant American Express BCRs Entity acting as Data Importer (including any requirements to disclose Personal Data or measures authorising access by public authorities), do not prevent it from fulfilling its obligations under these BCRs. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society are not in contradiction with these BCRs, where they safeguard one of the following objectives (as listed in Article 23(1) of the GDPR):

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the European Union or of a Member State, in particular an important economic or financial interest of the European Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

In assessing the laws and practices of the Third Country which may affect compliance with the provisions of the BCRs, the American Express BCRs Entities have taken (and will take) due account of, in particular, the following elements:

i. The specific circumstances of the Transfers or set of Transfers, and of any envisaged onward Transfers within the same Third Country or to another Third Country, including:

- purposes for which the data are transferred and processed (e.g. HR, storage, IT support);
- types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
- economic sector in which the Transfer or set of Transfers occur;
- categories and format of the Personal Data transferred;
- location of the Processing, including storage; and
- transmission channels used.

ii. The laws and practices of the Third Country that are relevant in light of the circumstances of the Transfers, including those requiring the disclosure of Personal Data to public authorities or authorising access by such authorities and those providing for access to such data during transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.

iii. Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCRs, including measures applied

during the transmission and to the Processing of the Personal Data in the Third Country of destination.

Where any safeguards in addition to those envisaged under the BCRs should be put in place, AEESA, the DPO and American Express' network of relevant privacy specialists will be informed and involved in such assessment.

The Data Exporter should appropriately document such assessment, as well as the supplementary measures selected and implemented. The Data Exporter will make the documentation available to the Competent Supervisory Authorities upon request.

If any Data Importer has reasons to believe that, during its membership of these BCRs and when using these BCRs as a tool for Transfers, it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCRs (including following a change in the laws in the Third Country or a measure (such as a disclosure request)), the Data Importer will promptly notify the Data Exporter and also provide such information to AEESA. The following process will also be followed:

- The Data Importer will promptly notify the Data Exporter of the above and also provide this information to AEESA.
- Upon verification of such notification, the Data Exporter, along with AEESA, the DPO and American Express' network of relevant privacy specialists, shall promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or its Data Importer, in order to enable them to fulfil their obligations under the BCRs. This process shall also apply if the Data Exporter has reasons to believe that its Data Importer can no longer fulfil its obligations under the BCRs.
- Where the Data Exporter, along with AEESA and the DPO and American Express' network of relevant privacy specialists, assesses that the BCRs – even if accompanied by supplementary measures – cannot be complied with for a Transfer or set of Transfers, or if instructed to do so by the Competent Supervisory Authority (or Authorities), the Data Exporter shall suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.
- Following such a suspension, the Data Exporter will end the Transfer or set of Transfers if the BCRs cannot be complied with and compliance with the BCRs is not restored within one month of suspension. In this case, Personal Data that has been transferred prior to the suspension, and any copies thereof,

should, at the choice of the Data Exporter, be returned to it or destroyed in their entirety.

- AEESA and the DPO and American Express' network of relevant privacy specialists will inform all other American Express BCRs Entities of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other American Express BCRs Entities or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

Each Data Exporter will monitor, on an ongoing basis, and where appropriate in collaboration with its Data Importers, developments in the Third Countries to which the Data Exporters have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers.

11.2 Data Importer's obligations in the event of government access requests

In addition to, and without prejudice to the Data Importer's obligation to inform its Data Exporter of its inability to comply with the provisions in these BCRs (as set out in Section 11.1 above), the Data Importer will promptly notify the Data Exporter and, where possible, the Data Subject (if necessary, with the help of the Data Exporter) if it:

a) receives a legally binding request by a public authority under the laws of the Third Country, or of another third country, for disclosure of Personal Data transferred pursuant to these BCRs. Such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; and/or

b) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these BCRs in accordance with the laws of the country of destination. In this case, such notification will include all information available to the Data Importer.

If prohibited from notifying the Data Exporter and / or the impacted Data Subject(s), the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible and as soon as possible. The Data Importer will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

The Data Importer will provide the Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCRs and shall make it available to the Competent Supervisory Authorities upon request.

The Data Importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity. In these circumstances:

- The Data Importer will, under the same conditions, pursue possibilities of appeal.
- When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter and make such documentation available to the Competent Supervisory Authorities upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, Transfers of Personal Data by an American Express BCRs Entity to any public authority will not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society. This limitation shall apply to any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body.

11.3. Relationship between national laws and the EU BCRs

Where the Applicable Data Protection Legislation requires a higher level of protection for Personal Data, those data protection laws will take precedence over these BCRs.

12. NON-COMPLIANCE WITH THE EU BCRs

All American Express BCRs Entities agree that:

- No Transfer will be made to another American Express BCRs Entity unless that entity is effectively bound by the BCRs and can deliver compliance.
- The Data Importer will promptly inform the Data Exporter if it is unable to comply with the BCRs, for whatever reason, including the situations further described under Section 11 above.
- Where the Data Importer is in breach of the BCRs or unable to comply with them, the Data Exporter will suspend the Transfer.
- The Data Importer will, at the choice of its Data Exporter, immediately return or delete the Personal Data that has been transferred under the BCRs in its entirety, in circumstances where:
    - the Data Exporter has suspended the Transfer, and compliance with the BCRs is not restored within a reasonable time, and in any event within one month of suspension; or
    - the Data Importer is in substantial or persistent breach of the BCRs; or
    - the Data Importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the BCRs.

The above obligations will apply to any copies of the Personal Data and the Data Importer will certify the deletion of such data to the Data Exporter.

Until the data is deleted or returned, the Data Importer will continue to ensure compliance with the BCRs.

If local laws apply to the Data Importer that prohibits the return or deletion of the Transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with the BCRs and will only Process the Personal Data to the extent and for as long as is required under that local law.

13. TERMINATION

If a Data Importer ceases to be bound by the BCRs, such American Express BCRs Entity may keep, return, or delete the Personal Data received under the BCRs, provided that, if the Data Importer and the relevant Data Exporter agree that the Personal Data may be kept by that Data Importer, the Data Importer must maintain the protection of such Personal Data in accordance with the requirements set out in Chapter V (transfers of personal data to third countries or international organisations) of the GDPR, namely:

- The Data Importer will not undertake any Transfer of such Personal Data unless there is an appropriate safeguard in place;

- The Data Importer shall continue to comply with the BCRs with respect to such Personal Data, in order to maintain the protection of the data; and

- The Data Importer shall only Process the Personal Data to the extent and for as long as is required for the purpose for which such data is retained by the Data Importer.

14. UPDATES TO THE EU BCRs

We may update the terms of our BCRs to, for instance, consider modifications of the regulatory environment or the company structure. We commit to report changes to our BCRs without undue delay to all American Express BCRs Entities.

Any changes to the BCRs or to the list of American Express BCRs Entity will be reported once a year to the relevant Supervisory Authorities, via the Lead Supervisory Authority with a brief explanation of the reasons for the updates. The relevant Supervisory Authorities will also be notified in circumstances where no changes have been made.

Where a modification would possibly affect the level of the protection offered by these BCRs or significantly affect these BCRs (e.g. changes to the binding character, change of the American Express BCRs Entity responsible for breaches of the BCRs, etc.), it will be promptly communicated to the relevant Supervisory Authorities in advance, via the Lead Supervisory Authority, with a brief explanation of the reasons for the update. In this case, the Supervisory Authority will also assess whether the changes made require a new approval.

American Express has identified a team (its Global Privacy Office function) that keeps a fully updated list of the American Express BCRs Entities and keeps track of

and records any updates to the rules and provides the necessary information to the Data Subjects or, upon request, to Competent Supervisory Authorities. In addition, the American Express BCRs Entities will not make any Transfer to a new American Express BCRs Entity until this new entity is effectively bound by these BCRs and can deliver compliance.

APPENDIX 1 – NATURE AND PURPOSES OF PERSONAL DATA TRANSFERRED WITHIN THE SCOPE OF THE BCRs

Type of processing and purposes	Categories of Personal Data
Categories of Data Subject: Employees	
To Process Employee data for the purpose of emergency medical care	Email address; Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Telephone/personal cellular/fax
For tax purposes, where laid down by Member State law to which the relevant Data Controller is subject	Children information (age/gender contact info, etc.); Disability / Regulation-Driven Accommodation Status; Income; Legal judgements or proceedings; Nationality; Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Challenge / Security question and/or answers; Green/Alien resident card number; National ID; Social Security Number (Full/Partial/Scrambled); Children information (age/gender contact info, etc.); Legal judgements or proceedings; Membership or trade unions; Nationality; Receipt of child support, alimony or separate maintenance; Receipt of public assistance (i.e. welfare benefits); Age; Band level; Charitable contribution ROC data; Date of birth; Education level; Email address; Employee ID/Customer Employment ID; Employer name; Employment history or status; Family with children indicator; Individual's name (last + first name/initial); Leave of absence type; Marital or familial status; Payment history; Retirement date; Separation date; Street Address; Tax ID Number; Telephone/personal cellular/fax

Type of processing and purposes	Categories of Personal Data
To perform our obligations under your employment contract, for example, to process and pay your salary and manage your employee benefits (including medical, insurance and pensions) and fulfil the legal obligations created within your employment contract.	Separation date; Retirement Date; Children information (age/gender contact info, etc.); Disability / Regulation-Driven Accommodation Status; Legal judgements or proceedings; Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Challenge / Security question and/or answers; Green/Alien resident card number; Children information (age/gender contact info, etc.); Legal judgements or proceedings; Membership or trade unions; Receipt of child support, alimony or separate maintenance; Receipt of public assistance (i.e. welfare benefits); Charitable contribution ROC data; Employment history or status; Family with children indicator;; Payment history; Account number (Full/Partial/Scrambled) - Other Payment Institutions; Driver's license number; National ID; Social Security Number (Full/Partial/Scrambled); Income; Nationality; Age; Band level; Date of birth; Education level; Email address; Employee ID/Customer Employment ID; Employer name; Gender; Ethnicity or race; Individual's name (last + first name/initial); Leave of absence type; Marital or familial status; Occupation; Retirement date; Separation date; Street Address; Tax ID Number; Telephone/personal cellular/fax; Username
Processing employee work-related claims and litigation.	Passport Number; Nationality; Band level; Date of birth; Email address; Employee ID/Customer Employment ID; Employment history or status; Individual's name (last + first name/initial); Photograph; Street Address; Telephone/personal cellular/fax; Biometric information; Children information (age/gender contact info, etc.)
Conducting performance reviews and determining performance requirements.	Band level; Education level; Employee ID/Customer Employment ID; Employment history or status; Gender; Individual's name (last + first name/initial); Performance rating; Occupation; Separation date.

Type of processing and purposes	Categories of Personal Data
To protect, safeguard and monitor the health, safety, and security of our employees.	Protected Health Information (PHI); Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Email address; Band level; Employer name
To administer and manage your benefits and any other incentives or programs you participate in as an employee, including the administration and/or request of restaurant vouchers and/or electronic card food vouchers.	Passport Number; Employee ID/Customer Employment ID; Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Children information (age/gender contact info, etc.); Authorized agent/Program Administration information; Customer status; Employer name; Payment history; Street Address; Account number (Full/Partial/Scrambled) - Other Payment Institutions; Driver's license number; National ID; Social Security Number (Full/Partial/Scrambled); Disability / Regulation-Driven Accommodation Status; Income; Nationality; Information (PHI); Age; Band level; Date of birth; Education level; Email address; Employee ID/Customer Employment ID; Employer name; Employment history or status; Family with children indicator; Gender; Individual's name (last + first name/initial); Insurance policies; Leave of absence type; Marital or familial status; Occupation; Retirement date; Separation date; Street Address; Tax ID Number; Telephone/personal cellular/fax; Username
To ensure network, office, and information security, including preventing unauthorized access to our systems and office locations and to safeguard our employees, business interests and property and prevent fraud, including by facilitating access to and monitoring activity on our premises and systems and compliance with internal policies.	Biometric information; Band level; Email address; Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Photograph
For training, education and development purposes or	Band level; Email address. Device/app data; Employee ID/Customer Employment ID; Employer

Type of processing and purposes	Categories of Personal Data
requirements, including the creation of an employee profile to facilitate these activities.	name; IP Address; Individual's name (last + first name/initial);
To verify your educational credentials (for example, if you earn a qualification or certification during your employment with us).	Individual's name (last + first name/initial); Employment history or status; Date of birth.
For our internal business and management purposes, including for the purpose of ensuring compliance with internal American Express policies, budgeting, forecasts, planning and related analysis and management (which may include the creation of reports for analysis, which may be aggregated and anonymized).	Account Number (Full/Partial/Scrambled) - AMEX
To run, manage and/or reorganize our business, assets, and operations (including in anticipation of any proposed business sale, merger, or divestiture).	Band level; Diversity data; Email address; Employee ID/Customer Employment ID; Employment history or status; Gender; Individual's name (last + first name/initial); IP Address; Occupation; Opinions captured; Performance rating; Separation date
To inform and manage our internal company policies, office utilization and real estate capacity and to improve working conditions for our employees (which may include the creation of reports for analysis, which may be aggregated and anonymized).	Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Email address; Band level; Employer name
To record and monitor customer calls for the following purposes: training, quality, compliance, fraud prevention and complaint handling.	Account Number (Full/Partial/Scrambled) Account number (Full/Partial/Scrambled) - Other Payment Institutions; National ID; PIN/pass code/password; Social Security Number (Full/Partial/Scrambled); Income; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date;

Type of processing and purposes	Categories of Personal Data
	Customer purchase/ transaction data; Date of birth; Email address; Individual's name (last + first name/initial); Street Address; Telephone/personal cellular/fax
For accounting and auditing purposes.	Income; Age; Band level; Date of birth; Employee ID/Customer Employment ID; Employer name; Employment history or status; Individual's name (last + first name/initial); Retirement date; Separation date
To ensure equality of opportunity and treatment in accordance with policy and equal opportunities legislation and for global diversity, equality, and inclusion initiatives.	Ethnicity or race; Age- Band level; Date of birth; Diversity data; Email address; Employee ID/Customer Employment ID; Employer name; Gender; Individual's name (last + first name/initial); Occupation
For management and analysis of employee and business expenses and technologies administration (e.g., American Express device management).	Account Number (Full/Partial/Scrambled) - AMEX; Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Email address; Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Street Address; Tax ID Number
To comply with applicable laws and undertake sanctions screening, including where required with respect to judicial or administrative orders regarding individual employees and/or for regulatory submissions and/or to conduct internal investigations.	Nationality; Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; Green/Alien resident card number; National ID; Passport Number; Social Security Number (Full/Partial/Scrambled); Authorized agent/Program administration information; Card type (e.g. Emboss code) / Service code (card parameters); Customer purchase/ transaction data; Customer status; Date of birth; Email address; Employer name; Gender; Individual's name (last + first name/initial); IP Address; Non-driver's ID; Occupation; Payment history; Sole trader/proprietor business data; Sole trader/proprietor demographic data; Street Address; Tax ID Number; Telephone/personal cellular/fax; Age; Ticket or travel record locator; Political Affiliations/Opinions; Mother's maiden name

Type of processing and purposes	Categories of Personal Data
To cooperate with regulators, law enforcement and other authorities	Individual's name (last + first name/initial); Band level; Employee ID/Customer Employment ID; Email address; Telephone/personal cellular/fax; Street Address
To market and send you promotions and offers about our products, services, and employee incentives	Band level; Diversity data; Email address; Only for Leaders - Employee ID/Customer Employment ID; Employment history or status; Gender; Individual's name (last + first name/initial) Only for Leaders; IP Address; Occupation; Opinions captured; Performance rating; Separation date;
To monitor and report on workplace diversity and to develop initiatives promoting a more inclusive workplace, we may process Personal Data relating to your sexual orientation or disability status	Ethnicity or race- Age- Band level- Date of birth- Diversity data- Email address- Employee ID/Customer Employment ID- Employer name- Gender- Individual's name (last + first name/initial)- Occupation
Biometric data for the purpose of identifying you and to grant you access to office locations.	Biometric information; Band level; Email address; Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Photograph
To comply with health and safety law and equal opportunities legislation, we may process Personal Data relating to your health or condition (for example, information relating to any disabilities you may have)	Protected Health Information (PHI); Employee ID/Customer Employment ID; Individual's name (last + first name/initial); Email address; Band level; Employer name
We may process Personal Data relating to your health or condition as part of sickness absence or workplace accident management, to administer benefits and to ensure you receive the correct entitlements and support from us	Account number (Full/Partial/Scrambled) - Other Payment Institutions; Driver's license number; National ID; Social Security Number (Full/Partial/Scrambled); Children information (age/gender contact info, etc.); Disability / Regulation-Driven Accommodation Status; Income; Nationality; Protected Health Information (PHI); Age; Band level; Date of birth; Education level; Email address; Employee ID/Customer Employment ID; Employer name; Employment history or status; Family with children indicator; Gender; Individual's name (last + first name/initial);

Type of processing and purposes	Categories of Personal Data
	Insurance policies; Leave of absence type; Marital or familial status; Occupation; Retirement date; Separation date; Street Address; Tax ID Number; Telephone/personal cellular/fax; Username
We may also process Personal Data relating to criminal convictions and offences data in certain circumstances including where we are legally required to respond to requests from law enforcement officers, where we conduct sanctions screening and in the context of legal claims where we need to establish, exercise, or defend our legal rights	Individual's name (last + first name/initial); Employment history or status; Date of birth.
Categories of Data Subject: Customers	
Process applications for cards, account, or other products or to manage a customer's existing accounts	Date of birth; Email address; Individual's name (last + first name/initial); Nationality; Telephone/personal cellular/fax; Mother's maiden name; Passport Number;
To report certain suspicious transactions to the competent authorities under anti-money-laundering rules or as required by law to perform due diligence on Customers before approving their applications	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account number (Full/Partial/Scrambled) - Other Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; Green/Alien resident card number; National ID; Passport Number; Social Security Number (Full/Partial/Scrambled); Criminal record; Income; Legal judgements or proceedings; Membership or trade unions; Nationality; Age; Band level; Card type (e.g. Emboss code) / Service code (card parameters); Charitable contribution ROC data; Credit card expiration date; Customer purchase/ transaction data; Customer service record; Customer status; Date of birth; Education level; Educational or professional affiliations; Email address; Employee badge/profile photo; Employee ID/Customer Employment ID; Employer name; Employment history or status; Gender; Individual's name (last + first name/initial); IP

Type of processing and purposes	Categories of Personal Data
	Address; Membership Reward (MR) number; Mother's maiden name; Non-driver's ID; Occupation; Payment history; Performance rating; Personal directory data; Photograph; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Street Address; Tax ID Number; Telephone/personal cellular/fax; Ticket Number or travel record locator
To comply with our regulatory obligations when reviewing your application	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; National ID; Passport Number; Social Security Number (Full/Partial/Scrambled); Income; Age; Customer status; Date of birth; Email address; Employer name; Credit scoring results; Gender; Individual's name (last + first name/initial); Mother's maiden name; Occupation; Payment history; Street Address; Tax ID Number; Telephone/personal cellular/fax
To administer and manage your account and provide our services to you and/or your company, such as whether to process, approve and complete individual transactions	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Email address; Individual's name (last + first name/initial); Driver's license number; National ID; PIN/pass code/password; Income; Legal judgements or proceedings; Age; Credit card expiration date; Date of birth; Employer name; Employment history or status; Credit scoring results; Sole trader/proprietor business data; Street Address; Tax ID Number; Telephone/personal cellular/fax; Challenge / Security question and/or answers; Online unique identifier (including cookies); Customer purchase/ transaction data; Marketing and privacy preferences (e.g. DNC); Occupation; P(P1) Authorized agent/Program Administration information; Customer status; Customer service record; High value card member indicator; Insurance policies; Marital or familial status; Membership Reward (MR) number; Payment history; Records of Charge (ROC) for Financial

Type of processing and purposes	Categories of Personal Data
	Services/ Government / Healthcare; Sole trader/proprietor demographic data; Username; Customer service record; Customer status; Mother's maiden name; Partner account number (including FF number);
To manage any benefits, insurance, travel, or other corporate programmes in which you or your company is enrolled	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Customer purchase/ transaction data; Customer service record; Customer status; Date of birth; Email address; High value card member indicator; Marketing and privacy preferences (e.g. DNC); Membership Reward (MR) number; Mother's maiden name; Partner account number (including FF number); Street Address; Telephone/personal cellular/fax; Username
To provide you with the location-based services you requested (if any)	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; National ID; Age; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Customer status; Date of birth; Email address; Gender; High value card member indicator; Individual's name (last + first name/initial); Partner account number (including FF number); Street Address; Telephone/personal cellular/fax; Token/GUID/PAR
To communicate with you through email, SMS, or any other electronic methods, by post and/or phone about your accounts, products, and services for legal, regulatory, or servicing purposes (such as updating you about features attached to your products or services)	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Telephone/personal cellular/fax; Ticket Number or travel record locator; Age; Customer purchase/ transaction data; Date of birth; Disability / Regulation-Driven Accommodation Status; Diversity data; Education level; Email address; Employer name; Employment history or status; Family with children indicator; Credit scoring results; Gender; High value card member indicator; Income; Individual's name (last + first name/initial); IP Address; Marital or familial status; Occupation; Online

Type of processing and purposes	Categories of Personal Data
	unique identifier (including cookies); Opinions captured; Photograph; Real-time / precise/geo-location information; Sexual orientation; Street Address; National ID; Authorized agent/Program Administration information; Credit card expiration date; Customer status; Customer service record; Insurance policies; Marital or familial status; Marketing and privacy preferences (e.g. DNC); Membership Reward (MR) number; Payment history; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Sole trader/proprietor business data; Sole trader/proprietor demographic data; Tax ID Number; Username
By providing a more appropriate service and/or protecting your best interests by making reasonable adjustments, such as sending or providing you information in an appropriate format	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Email address; Individual's name (last + first name/initial); Driver's license number; National ID; PIN/pass code/password; Income; Legal judgements or proceedings; Age; Credit card expiration date; Date of birth; Employer name; Employment history or status; Credit scoring results; Sole trader/proprietor business data; Street Address; Tax ID Number; Telephone/personal cellular/fax; Challenge / Security question and/or answers; Online unique identifier (including cookies); Customer purchase/ transaction data; Marketing and privacy preferences (e.g. DNC); Occupation; P(P1) Authorized agent/Program Administration information; Customer status; Customer service record; High value card member indicator; Insurance policies; Marital or familial status; Membership Reward (MR) number; Payment history; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Sole trader/proprietor demographic data; Username; Customer service record; Customer status;

Type of processing and purposes	Categories of Personal Data
	Mother's maiden name; Partner account number (including FF number);
To service and manage any benefits and insurance programmes provided along with the products or services that you requested	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Customer purchase/ transaction data; Customer service record; Customer status; Date of birth; Email address; High value card member indicator; Marketing and privacy preferences (e.g. DNC); Membership Reward (MR) number; Mother's maiden name; Partner account number (including FF number); Street Address; Telephone/personal cellular/fax; Username
When interacting with some of our business partners available in your card benefits programme, to connect you to your Membership Rewards account (if applicable) and, depending on your card product, enable you to use Membership Rewards points to pay for products or services with a business partner	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions
To carry out checks for the purpose of keeping your account and Personal Data secure, detecting, and preventing fraud or criminal activity (including the review and approval of individual transactions) and to check your identity before providing services to you (including through "know your customer" screening and monitoring)	Account Number (Full/Partial/Scrambled) - AMEX; Social Security Number (Full/Partial/Scrambled); Driver's license number; National ID; Authorized agent/Program Administration information; Date of birth; Email address; Individual's name (last + first name/initial); Tax ID Number
To answer questions submitted to us by you, respond to your requests and manage and deal with any complaints you may have.	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card parameters); Email address; Individual's name (last + first name/initial); Driver's license number; National ID; PIN/pass code/password; Income; Legal judgements or

Type of processing and purposes	Categories of Personal Data
	proceedings; Age; Credit card expiration date; Date of birth; Employer name; Employment history or status; Credit scoring results; Sole trader/proprietor business data; Street Address; Tax ID Number; Telephone/personal cellular/fax; Challenge / Security question and/or answers; Online unique identifier (including cookies); Customer purchase/ transaction data; Marketing and privacy preferences (e.g. DNC); Occupation; P(P1) Authorized agent/Program Administration information; Customer status; Customer service record; High value card member indicator; Insurance policies; Marital or familial status; Membership Reward (MR) number; Payment history; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Sole trader/proprietor demographic data; Username; Customer service record; Customer status; Mother's maiden name; Partner account number (including FF number);
To protect our business interests, recover debt and exercise other rights we have under any contract with you	Account Number (Full/Partial/Scrambled) - AMEX. Challenge / Security question and/or answers; Driver's license number; National ID; PIN/pass code/password; Income; Legal judgements or proceedings; Age; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Date of birth; Email address; Employer name; Employment history or status; Credit scoring results; Individual's name (last + first name/initial); Sole trader/proprietor business data; Street Address; Tax ID Number; Telephone/personal cellular/fax; Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Customer purchase/ transaction data; Gender; High value card member indicator; Occupation; Payment history; Proprietary predictive Credit score algorithms and those relating to Intellectual Property.

Type of processing and purposes	Categories of Personal Data
To establish, exercise, or defend legal rights or claims and assist in dispute resolution	Individual's name (last + first name/initial); Band level; Employee ID/Customer Employment ID; Email address; Telephone/personal cellular/fax; Street Address
To develop and improve our products and services, including for the purpose of better understanding our customers, their needs, preferences, and behaviours; place you in groups with similar customers to deliver products or services which may be more suitable for you or suit your preferences; and assess and analyse whether our ads, promotions and offers are effective	Account Number (Full/Partial/Scrambled) - AMEX; Customer purchase/ transaction data; High value card member indicator; Individual's name (last + first name/initial)
To help us better understand your financial circumstances and behaviour so that we can make decisions about how we manage your existing accounts and what other products or services can be extended to you	Account Number (Full/Partial/Scrambled) - AMEX; Customer purchase/ transaction data; Credit scoring results; Proprietary predictive Credit score algorithms and those relating to Intellectual Property; Income; Age; Mortgage or other loan information; Payment history
To check we have carried out your instructions correctly, to develop and improve our services and for training and quality purposes	Children information (age/gender contact info, etc.). Disability / Regulation-Driven Accommodation Status. Account Number (Full/Partial/Scrambled) - AMEX. Nationality. Age; Card type (e.g. Emboss code) / Service code (card parameters); Date of birth. Telephone/personal cellular/fax; Email address; Challenge / Security question and/or answers. Passport Number. Protected Health Information (PHI). Authorized agent/Program Administration information; Credit card expiration date. Gender. Individual's name (last + first name/initial); Street Address.

Type of processing and purposes	Categories of Personal Data
	Ticket Number or travel record locator; National ID; Credit card expiration date; Customer purchase/ transaction data; Customer status; Customer service record; High value card member indicator; Insurance policies; Marital or familial status; Marketing and privacy preferences (e.g. DNC); Membership Reward (MR) number; Occupation; Payment history; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Sole trader/proprietor business data; Sole trader/proprietor demographic data; Tax ID Number; Username; Employee ID/Customer Employment ID;; Telephone/personal cellular/fax; Mother's maiden name; Partner account number (including FF number);
To record and monitor calls for the following purposes: training, quality, compliance, fraud prevention and complaint handling	Challenge / Security question and/or answers. Driver's license number. Passport Number. Children information (age/gender contact info, etc.). Disability / Regulation-Driven Accommodation Status; Nationality; Protected Health Information (PHI). Age. Authorized agent/Program Administration information. Gender. Ticket Number or travel record locator Account Number (Full/Partial/Scrambled) - AMEX. Account number (Full/Partial/Scrambled) - Other Payment Institutions. National ID; PIN/pass code/password. Social Security Number (Full/Partial/Scrambled); Income; Card type (e.g. Emboss code) / Service code (card parameters). Credit card expiration date. Customer purchase/ transaction data. Date of birth; Email address. Individual's name (last + first name/initial). Street Address. Telephone/personal cellular/fax

Type of processing and purposes	Categories of Personal Data
For specific purposes relating to Open Banking	Account Number (Full/Partial/Scrambled) – AMEX; Account number (Full/Partial/Scrambled); Other Payment Institutions; Individual's name (last + first name/initial); Customer purchase/ transaction data
To conducting testing (to ensure security and when we update our systems), website administration, information technology system support and development and to safeguard the security of your Personal Data	PIN/pass code/password; Device/app data; Email address; Telephone/personal cellular/fax; Employee ID/Customer Employment ID; Token/GUID/PAR; Username; IP Address
To develop and refine our risk management policies, models and procedures for applications and customer accounts, relying upon information in your application or relating to your Creditworthiness (including any information provided by third parties), fraud risk and account history (if applicable)	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; National ID; Passport Number; Social Security Number (Full/Partial/Scrambled); Income; Age; Customer status; Date of birth; Email address; Employer name; Credit scoring results; Gender; Individual's name (last + first name/initial); Mother's maiden name; Occupation; Payment history; Street Address; Tax ID Number; Telephone/personal cellular/fax
To inform our collection practice and share information with collection agencies and fraud management agencies	Account Number (Full/Partial/Scrambled) - AMEX; Challenge / Security question and/or answers; National ID; PIN/pass code/password; Social Security Number (Full/Partial/Scrambled); Income; Legal judgements or proceedings; Receipt of child support, alimony or separate maintenance; Receipt of public assistance (i.e. welfare benefits); Age; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Credit card security code; Customer purchase/ transaction data; Customer status; Date of birth; Email address; Employer name; Credit scoring results
To conduct research and analytics, including allowing you to give feedback by rating and	Account Number (Full/Partial/Scrambled) - AMEX; Card type (e.g. Emboss code) / Service code (card

Type of processing and purposes	Categories of Personal Data
reviewing our products and services and those of our business partners and to produce data analytics, statistical research, and reports on an aggregated basis	parameters); Customer purchase/ transaction data; Email address; Payment history; Username
To prepare reports and statistics to enable your company to uphold an effective administration and procurement policy (this may also include information on outstanding debt)	Individual's name (last + first name/initial); Date of birth; Nationality; Occupation; Telephone/personal cellular/fax; Email address; Street Address;
To cooperate with regulators, law enforcement and other authorities.	Band level; Challenge / Security question and/or answers; Online unique identifier (including cookies); PIN/pass code/password; Real-time / precise/geo-location information; TRACK Data; Credit card expiration date; Customer purchase/ transaction data; Payment history; Records of Charge (ROC) for Financial Services/ Government / Healthcare; Gender; Place of birth Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; Green/Alien resident card number; National ID; Passport Number; Social Security Number (Full/Partial/Scrambled); Income; Nationality; Authorized agent/Program Administration information; Customer status (report only default); Customer status; Date of birth; Email address; Employee ID/Customer Employment ID; Employer name; Employment history or status; Individual's name (last + first name/initial); IP Address; Non-driver's ID; Occupation; Sole trader/proprietor business data; Sole trader/proprietor demographic data; Street Address; Tax ID Number; Telephone/personal cellular/fax
To comply with legal and regulatory obligations (such as performing due diligence on you before approving your application)	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; Account Number (Full/Partial/Scrambled) - AMEX; Driver's license number; National ID; Passport Number; PIN/pass code/password; Income; Nationality; Age; Assets/net worth; Authorized

Type of processing and purposes	Categories of Personal Data
	agent/Program Administration information; Card type (e.g. Emboss code); Customer Status; Date of birth; Device/app data; Education level; Educational or professional affiliations; Email Address; Employer name; Employment history or status; Individual's name (last + first name/initial); IP Address; Marketing and privacy preferences (e.g. DNC); Membership Reward (MR) number; Mortgage or other loan information; Non-driver's ID; Occupation; Other government issued ID; Partner account number (including FF number); Proprietary/predictive Credit scores algorithms and those relating to Intellectual Property; Sole trader/proprietor business Data; Sole trader/proprietor demographic data; Street Address; Telephone/personal cellular/fax
To market products and services which we think you will be interested in based on your relationship with us (by email, SMS, or telephone (for example - if you call us)). We would do this only where the law allows for this based on opt-out	Account Number (Full/Partial/Scrambled) - AMEX; Age; Card type (e.g. Emboss code) / Service code (card parameters); Customer purchase/ transaction data; Date of birth; Disability / Regulation-Driven Accommodation Status; Diversity data; Education level; Email address; Employer name; Employment history or status; Family with children indicator; Credit scoring results; Gender; High value card member indicator; Income; Individual's name (last + first name/initial); IP Address; Marital or familial status; Occupation; Online unique identifier (including cookies); Opinions captured; Photograph; Real-time / precise/geo-location information; Sexual orientation; Street Address; Telephone/personal cellular/fax
To advertise, market and send you promotions and offers about products and services for or from the American Express Group (i.e., any affiliate, subsidiary, joint venture, and any company owned or controlled by our parent company) and our business	Account Number (Full/Partial/Scrambled) - Other Non-Payment Institutions; National ID; Age; Card type (e.g. Emboss code) / Service code (card parameters); Credit card expiration date; Customer status; Date of birth; Email address; Gender; High value card member indicator; Individual's name (last + first name/initial); Partner account number (including FF number); Street

Type of processing and purposes	Categories of Personal Data
partners, including to present content that is personalised and tailored to your preferences and interests, including targeted advertising across multiple devices or showing you offers in your Manage Your Card Account (MYCA) environment	Address; Telephone/personal cellular/fax; Token/GUID/PAR
Biometric data for the purpose of identifying you, for security verification and to detect and prevent fraud	Biometric information; Photograph;

APPENDIX 2 –AMERICAN EXPRESS BCRs ENTITIES

BCR Legal Entities as of July 2024						
Company Name	Country	Headquarters' Address	Type of Entity	Main Activity	Importer / Exporter	Company Number
American Express (India) Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Majority or Wholly Owned Subsidiary	Provides support services for other Amex companies	Data Importer / Data Exporter	U74899DL1994PTC059865
American Express (Malaysia) SDN. BHD.	Malaysia	Level 14, Menara Prestige, No.1, Jalan Pinang, 50450 Kuala Lumpur, Malaysia	Majority or Wholly Owned Subsidiary	Customer servicing company	Data Importer / Data Exporter	46752-M
American Express (Thai) Company Limited	Thailand	S.P.Building, 388 Phaholyothin Road, Samsennai, Phayathai, Bangkok, 10400, Thailand	Majority or Wholly Owned Subsidiary	Charge and credit card issuer	Data Importer / Data Exporter	105524019341,00
American Express Argentina S.A.	Argentina	Arenales 707, Mezzanine, Ciudad de Buenos Aires, Buenos Aires, C1061AAA, Argentina	Majority or Wholly Owned Subsidiary	Charge and credit card issuer	Data Importer / Data Exporter	161972
American Express Australia Limited	Australia	Level 1, 12 Shelley Street, Sydney NSW 2000, Australia	Majority or Wholly Owned Subsidiary	Merchant servicing company	Data Importer / Data Exporter	108 952 085
American Express Business Solutions (India) Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Majority or Wholly Owned Subsidiary	Customer servicing company	Data Importer / Data Exporter	U74140DL2015PTC277109

American Express Carte France SA	France	Bâtiment, Voyager, 8-10 rue Henri, Sainte Claire Deville, 92500, Rueil Malmaison, France	Majority or Wholly Owned Subsidiary	Charge and/or credit card issuer	Data Exporter	313 536 898 00015
American Express Company	United States of America	200 Vesey Street, New York NY 10285, United States	Parent entity	Merchant acquisition/ servicing	Data Importer / Data Exporter	13-4922250
American Express Company (Mexico) S.A. de C.V.	Mexico	Avenida Patriotismo #635, Col. Ciudad de los Deportes, Mexico City , Mexico, 03710, Mexico	Majority or Wholly Owned Subsidiary	Charge card issuer	Data Importer / Data Exporter	AEC810901298
American Express Credit Corporation	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Charge card receivables financing company	Data Importer / Data Exporter	11-1988350
American Express de Espana, S.A. (Sociedad Unipersonal)	Spain	Avda. Partenón 12-14, 28042, Madrid, Spain	Majority or Wholly Owned Subsidiary	Credit Card processing and servicing	Data Exporter	A-28521888
American Express Europe LLC	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Travel related services	Data Importer / Data Exporter	13-3147632
American Express Europe LLC - Branch - United Kingdom	United Kingdom	200 Vesey Street, New York NY 10285, United States	Branch Office	Foreign exchange services	Data Importer / Data Exporter	BR000897
American Express Europe, S.A.	Spain	Avda. Partenón 12-14, 28042, Madrid, Spain	Majority or Wholly Owned Subsidiary	Credit and charge card issuer	Data Exporter	A-82628041
American Express Europe, S.A. - Branch - Austria	Austria	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Card Issuing	Data Exporter	FN 495241 x
American Express Europe, S.A. - Branch - Belgium	Belgium	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	To provide financial services and other	Data Exporter	0776.653.759

				business related thereto.		
American Express Europe, S.A. - Branch - Denmark	Denmark	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Charge card issuer	Data Exporter	39560542
American Express Europe, S.A. - Branch - Finland	Finland	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Charge card issuer and Travel & Lifestyle Services	Data Exporter	2914139-2
American Express Europe, S.A. - Branch - Germany	Germany	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Credit and charge card issuer	Data Exporter	HRB 112342
American Express Europe, S.A. - Branch - Hungary	Hungary	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Credit and charge card issuer	Data Exporter	Not available
American Express Europe, S.A. - Branch - Ireland	Ireland	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Card Issuing	Data Exporter	908882
American Express Europe, S.A. - Branch - Netherlands	Netherlands	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Card Issuing	Data Exporter	71660275
American Express Europe, S.A. - Branch - Norway	Norway	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Charge card issuer and Travel & Lifestyle Services	Data Exporter	920 854 346
American Express Europe, S.A. - Branch - Poland	Poland	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Credit and charge card issuer	Data Exporter	KRS 0000733504
American Express Europe, S.A. - Branch - Sweden	Sweden	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Charge card issuer and Travel & Lifestyle Services	Data Exporter	516411-3911
American Express Group Services Limited	United Kingdom	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, United Kingdom	Majority or Wholly Owned Subsidiary	Administrative Office	Data Importer / Data Exporter	6613927
American Express Innovation Laboratories Limited - Branch - Singapore	Singapore	70 Sir John Rogerson'S Quay, Dublin 2, Ireland	Branch Office	Development of Software and applications	Data Importer / Data Exporter	T22FC0063A

American Express Insurance Services, Agente de Seguros, S.A. de C.V.	Mexico	Avenida Patriotismo #635, Col. Ciudad de los Deportes, Mexico City , Mexico, 03710, Mexico	Majority or Wholly Owned Subsidiary	Insurance Broker or Agent	Data Importer / Data Exporter	Not Applicable
American Express International (NZ), Inc.	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Merchant acquisition and servicing	Data Importer / Data Exporter	22-2155644
American Express International (NZ), Inc. - Branch - New Zealand	New Zealand	200 Vesey Street, New York NY 10285, United States	Branch Office	Merchant acquisition/ servicing	Data Importer / Data Exporter	867929
American Express International (Taiwan), Inc.	Taiwan	12th Floor No. 363, Fu- Hsing North Rd., Taipei, 105, Taiwan	Majority or Wholly Owned Subsidiary	Charge and credit card iss uer	Data Importer / Data Exporter	11825058
American Express International, Inc.	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Merchant servicing compa ny	Data Importer / Data Exporter	13-6115802
American Express International, Inc. - Branch - Australia	Australia	200 Vesey Street, New York NY 10285, United States	Branch Office	Data Processing Company	Data Importer / Data Exporter	ABN 15000618208
American Express International, Inc. - Branch - Germany	Germany	200 Vesey Street, New York NY 10285, United States	Branch Office	Services in the field of tourism and tourist travel	Data Exporter	11988
American Express International, Inc. - Branch - Hong Kong	Hong Kong	200 Vesey Street, New York NY 10285, United States	Branch Office	Credit and charge card issuer	Data Importer / Data Exporter	BRN - 02099825
American Express International, Inc. - Branch -	Japan	200 Vesey Street, New York NY 10285, United States	Branch Office	Credit, Charge card, Gift Card and Merchant Acquiring	Data Importer / Data	3841

Japan					Exporter	
American Express International, Inc. - Branch - Philippines	Philippines	200 Vesey Street, New York NY 10285, United States	Branch Office	Business Process Outsourcing Services - Customer Servicing	Data Importer / Data Exporter	F-552
American Express International, Inc. - Branch - Singapore	Singapore	200 Vesey Street, New York NY 10285, United States	Branch Office	Issue of charge & credit cards and provision of related financial services	Data Importer / Data Exporter	S68FC1878J
American Express International, Inc. - Branch - Switzerland	Switzerland	200 Vesey Street, New York NY 10285, United States	Branch Office	Services to AXP Affiliates	Data Importer / Data Exporter	CH-020.9.900.052-2
American Express Italia S.r.l.	Italy	Viale Alexandre, Gustave Eiffel 15, 00148, Roma, Italy	Majority or Wholly Owned Subsidiary	Card Issuing	Data Exporter	RM – 1521502
American Express Japan Co., Ltd.	Japan	4-1-1 Toranomon,, Minato- ku, Tokyo, 105-6920, Japan	Majority or Wholly Owned Subsidiary	Customer service company	Data Importer / Data Exporter	242951
American Express Limited	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Network licensing company	Data Importer / Data Exporter	13-2586873
American Express Marketing & Development Corp.	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Provides support services for other Amex companies	Data Importer / Data Exporter	20-3083109
American Express Overseas Credit Corporation Limited	Jersey	1st Floor, Le Gallais Building, 54 Bath Street, St. Helier, JE2 4SU, Jersey	Majority or Wholly Owned Subsidiary	Funding of cardmember receivables company	Data Importer/ Data Exporter	23072
American Express Payment Services Limited	United Kingdom	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX,	Majority or Wholly Owned Subsidiary	Merchant servicing company	Data Importer / Data Exporter	6301718

		United Kingdom				
American Express Payment Services Limited - Branch - Germany	Germany	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, United Kingdom	Branch Office	It is an empty shell which still holds liabilities vis-à-vis pensioners and former employees which cannot be transferred easily out.	Data Exporter	B 85745
American Express Payments Europe, S.L.	Spain	Avda. Partenón 12-14, 28042, Madrid, Spain	Majority or Wholly Owned Subsidiary	Merchant Acquiring and Servicing	Data Exporter	Not available
American Express Payments Europe, S.L. - Branch - France	France	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	839 240 520
American Express Payments Europe, S.L. - Branch - Germany	Germany	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	HRB 112344
American Express Payments Europe, S.L. - Branch - Italy	Italy	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	14778691007
American Express Payments Europe, S.L. - Branch - Netherlands	Netherlands	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	39929841
American Express Payments Europe, S.L. - Branch - Sweden	Sweden	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	516411-3598
American Express Payments Europe, S.L.U. - Branch - Austria	Austria	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	FN 493466 k
American Express Payments Europe, S.L.U. - Branch - Belgium	Belgium	Avda. Partenón 12-14, 28042, Madrid, Spain	Branch Office	Merchant Acquiring and Servicing	Data Exporter	0776.651.878

American Express Prepaid Card Management Corporation	United States of America	18850 N, 56th St, Phoenix Arizona 85054, United States	Majority or Wholly Owned Subsidiary	Card issuer	Data Importer/ Data Exporter	30-0524568
American Express Services Europe Limited	United Kingdom	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, United Kingdom	Majority or Wholly Owned Subsidiary	Charge and credit card issuer	Data Importer / Data Exporter	1833139
American Express Services Europe Limited - Branch - Germany	Germany	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, United Kingdom	Branch Office	Issuance of cards	Data Exporter	57783
American Express Services Europe Limited - Branch - Italy	Italy	Belgrave House, 76 Buckingham Palace Road, London, SW1W 9AX, United Kingdom	Branch Office	Financial Holding	Data Exporter	5090991000
American Express Services India Private Limited	India	MGF Metropolitan - Saket, 7th Floor, Office Block, District Centre Saket, New Delhi, 110017, India	Majority or Wholly Owned Subsidiary	Service Company for Affiliate	Data Importer / Data Exporter	U65921DL1999FTC101368
American Express TLS HK Limited	Hong Kong	Suites 1701-3 and 1712-14, 17/F, 12 Taikoo Wan Road, Taikoo Shing, Hong Kong, Hong Kong	Majority or Wholly Owned Subsidiary	Travel related services	Data Importer / Data Exporter	62391986
American Express Travel Related Services Company, Inc.	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Merchant Acquiring (Discount Revenue)	Data Importer / Data Exporter	13-3133497
American Express, spol. s r.o.	Czech Republic	Perlova 371/5, Prague 1, 110 00 , Czech Republic	Majority or Wholly Owned Subsidiary	Travel Agency	Data Exporter	571849

Amex Agenzia Assicurativa S.r.l.	Italy	Viale Alexandre, Gustave Eiffel 15, 00148, Roma, Italy	Majority or Wholly Owned Subsidiary	Insurance Broker or Agent	Data Exporter	10190130152
Amex Asesores de Seguros, S.A. (Sociedad Unipersonal)	Spain	Avda. Partenón 12-14, 28042, Madrid, Spain	Majority or Wholly Owned Subsidiary	Insurance Broker or Agent	Data Exporter	A-79770608

Amex Bank of Canada	Canada	2225 Sheppard Avenue East, Suite 100 , Toronto ON M2J 5C2, Canada	Majority or Wholly Owned Subsidiary	Foreign Bank other than a n FBO	Data Importer / Data Exporter	11937 6804 RC0001
Amex Canada Inc.	Canada	2225 Sheppard Avenue East, Suite 100 , Toronto ON M2J 5C2, Canada	Majority or Wholly Owned Subsidiary	Customer service company	Data Importer / Data Exporter	1627387
Amex General Insurance Agency, Inc.	Taiwan	12th Floor No. 363, Fu-Hsing North Rd., Taipei, 105, Taiwan	Majority or Wholly Owned Subsidiary	Insurance Broker or Agent	Data Importer/ Data Exporter	84306997
Amex Services, Inc.	United States of America	200 Vesey Street, New York NY 10285, United States	Majority or Wholly Owned Subsidiary	Customer services company	Data Importer / Data Exporter	13-6115803
Centurion Finance Limited	New Zealand	Jarden House, Level 5, 21 Queen Street, Auckland, 1010, New Zealand	Majority or Wholly Owned Subsidiary	Foreign exchange service company	Data Importer/ Data Exporter	104478
Centurion Finance Limited - Branch - Australia	Australia	Jarden House, Level 5, 21 Queen Street, Auckland, 1010, New Zealand	Branch Office	Foreign Exchange International Payment services	Data Importer/ Data Exporter	Not available
PT American Express Indonesia	Indonesia	The Plaza Complex Gondangdia, Lt 28 unit D, Jl. MH. Thamrin No.28 – 30, Menteng, Jakarta Pusat, 10350, Indonesia	Majority or Wholly Owned Subsidiary	Credit card issuer and pro vision of card support serv ices	Data Importer / Data Exporter	AHU-53498.AH.01.01.Tahun 2010

GLOSSARY

“AEESA” – means American Express Europe, S.A., located in Avenida Partenón 12 - 14, Madrid, 28042..

“American Express BCRs Entity” or “American Express BCRs Entities” or “We” or “Us” – means the American Express entity or entities which are bound by the Binding Corporate Rules, as set out in Appendix [2].

“American Express Company” - means American Express Company, located World Financial Center, 200 Vesey St., New York, NY 10285 USA.

“American Express Privacy Statements” - means the Cardmember Privacy Statement (for cardmembers), the Corporate Privacy Statement (for corporate Customers), the Online Privacy Statement (for Customers and website visitors), the Online Recruitment Privacy Statement (for potential Employees), or the Employee Privacy Notice (for current Employees), and other notices, terms and conditions (such as for merchants) which are applicable to the Data Subject’s relationship with American Express and as amended from time to time.

“Applicable Data Protection Legislation” – means the GDPR (and the national implementing legislations), the e-Privacy Directive 2002/58/EC (and the national implementing legislations), and any other data protection law and regulation applicable in the EEA (all the above as amended and replaced from time to time).

“Consent” – means any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

“Data Breach” or “Personal Data Breach” - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

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

"Data Exporter” – means the American Express BCRs Entity Transferring Personal Data under these BCRs.

"Data Importer" – means the American Express BCRs Entity located outside of the EEA receiving the Personal Data (directly or indirectly) from the Data Exporter.

"Data Protection Impact Assessment" – means an assessment of the impact of an envisaged Processing operation on the protection of Personal Data carried out where the Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

"Data Subject(s)" or "You" – refers to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, and whose Processing of Personal Data is subject to Applicable Data Protection Legislation and Transferred within the scope of these BCRs by an American Express BCRs Entity.

"Data Processor" - means the natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Data Controller.

"EEA" – means the European Economic Area, which includes all European Union countries as well as Iceland, Liechtenstein and Norway.

"GDPR" – means the General Data Protection Regulation 2016/679.

"Intra-Group Agreement" – means the intra-group agreement that binds American Express BCRs Entities to the BCRs.

"Personal Data" – means any information relating to a Data Subject.

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

"Profiling" –means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

“Special Categories of Data” – means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data Processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

“Supervisory Authority” or “Competent Supervisory Authority” – means an independent public authority related to a Data Exporter established in the EEA which is responsible for monitoring the application of Applicable Data Protection Laws.

“Third Country” – means a country outside of the EEA where the relevant American Express BCRs Entity is located.

“Transfer”– means any transfer of Personal Data from one company in the EEA, or otherwise subject to the GDPR, to another or onward transfer which would otherwise be restricted by the GDPR. A transfer is performed via any communication, copy or disclosure of Personal Data through a network, including remote access to a database or transfer from any medium to another.