Policy Name	**:**	**Global Employee Data Protection & Privacy Principles**
Country	**:**	**Global (All Countries)**
Policy Reference #	**:**	**L – 85.00**
Effective Date	**:**	**November 18, 2020**
Next Review Date	**:**	**November 18, 2023**
Responsible Functional Group	**:**	**Global Colleague Privacy Team**

1.0 HIGH-LEVEL DESCRIPTION AND PURPOSE

It is the policy of American Express ("the Company") to abide by the Employee Data Protection and Privacy Principles (Principles). These Principles set out the way that the Company will collect, use, store, share, transmit, delete, or otherwise process (collectively "process") employee personal data.

The content of this policy is reflective of the American Express Data Protection and Privacy Principles (herein after Privacy Principles or Principles) that apply to consumer and employee data. Any changes to the content are the result of changes to the core enterprise version of the Privacy Principles.

2.0 SCOPE

The standard of personal data protection set out in these Principles is used by the Company globally, providing adequate and consistent protection for the processing of employee personal data.

3.0 KEY DEFINITIONS

Personal Data: Sometimes called personally identifiable information (PII), refers to information, in any form, that identifies or can be used in combination with other information available to the Company to identify an individual and includes any information that is associated with an identified individual. See relevant market data protection policies for market-specific interpretations and requirements.

The information classification of Personal Data is subject to AXP Information Security Standards.

The Company: American Express ("AXP" or the "Company")

Processing: Refers to any action taken in relation to personal data and includes collecting, storing, altering, accessing, using, transferring, receiving, sharing or destroying personal data.

Colleague: Employee (Amex verbiage) (Covers Employment Candidate and Colleague personal data)

4.0 POLICY REQUIREMENTS / ELIGIBILITY

American Express Data Protection and Privacy Principles

Effective Date: March 15, 2018

The following Data Protection and Privacy Principles ("Principles") set out the way that American Express Company and its wholly owned direct and indirect subsidiaries ("American Express") will collect, use, store, share, transmit, delete or otherwise process (collectively "process") your personal data. Personal data means any information that relates to an identified or identifiable individual. The standard of personal data protection set out in these Principles will be used by American Express globally, providing adequate and consistent protection for the processing of your personal data. In these Principles, "you" and "your" means any individual customer or employee of American Express and any other individual whose personal data we process and "we", "us", "our" and "American Express Group" means American Express.

1- Collection
We will only collect personal data that is needed and by lawful and fair means.

2- Notice and Processing
Where it is not apparent from the employee relationship, we will tell employees how their personal data will be processed and which companies in the American Express Group are responsible for that processing. We will process employee personal data fairly and only for those purposes it has told employees about, for purposes permitted by employees, or as permitted by applicable law. In addition, employees may object to certain types of processing as expressly permitted by applicable law.

3- Choice
We collect personal data for employment related business purposes. Where law or contract requires your consent (a.k.a. choice) or the consent of an employee representative, we will comply with the law or contract.

4- Data Quality
We use appropriate technology and well-defined employee practices to process employee personal data promptly and accurately. We will not keep personal data longer than is necessary, except as otherwise required by applicable law.

5- Security and Confidentiality

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 permitted by applicable law. We refer to industry standards and uses reasonable administrative, technical, and physical security measures to protect your personal data from unauthorized access, destruction, use, modification, or disclosure. We require industry standard data security measures from those third parties who are authorized by us to process your personal data on our behalf.

6- Data Sharing

We only share your personal data with third parties where it is necessary to provide you with products or services or as part of our relationship with you, where we have previously informed or been authorized by you, in connection with our efforts to reduce fraud or criminal activity, or as permitted by law.

7- Openness and Data Access

If asked, we will inform you about how employee personal data is processed and the rights and remedies employees have under these Principles. You may inquire as to the nature of the personal data stored or processed about you by American Express. You will be provided access as is required by law in your country, regardless of the location of the data processing and storage. If any data is inaccurate or incomplete, you may request that the data be amended.

8- International Transfer

Where it is not apparent from the international products or services you require or the nature of your relationship with us, we will inform you if your personal data may be transferred outside of your country and ensure that such transfer is only performed in accordance with applicable law. Regardless of where your personal data is transferred, it is protected by these Principles.

9- Responsibility

Each company in the American Express Group and their employees may only process your personal data in accordance with these Principles. We conduct training and reviews of our compliance with these Principles. Employees who violate these Principles may be subject to disciplinary action, up to and including dismissal.

Employees are expected to report violations of these Principles and may do so to their leaders or Colleague Experience Group (CEG) representatives, to their business unit's compliance officer, to the General Counsel's Organization (GCO), to the Global Privacy Office, to the Global Compliance & Ethics or to the Amex Ethics Hotline (https://amex.ethicspoint.com/).

10- Accountability

You may enforce these Principles in your country against any company in the American Express Group that is responsible for your personal data, as a third party contractual beneficiary to these Principles. If you have a complaint that we have breached these Principles and have attempted in good faith to resolve the complaint through the employee complaints process, but the complaint was not resolved by us within a reasonable amount of time, then you may enforce these Principles against us. If you complain to your local data protection authority and the data protection authority finds that we have breached these Principles, we will abide by the findings of the data protection authority, but we reserve the right to challenge or appeal such findings. These Principles do

not affect any rights you have under applicable law, the requirements of any applicable regulatory data protection authority, or any other type of agreement that you may have with us.

5.0 ROLES AND RESPONSIBILITIES

Global Colleague Privacy Team

- disseminate this policy
- manage the content of this policy and make changes based on changes to the core enterprise version of the Global Data Protection and Privacy Principles

Employee/Colleague/Contractor responsibilities

Report violations of these principles to their leaders or CEG representatives, to their business unit's compliance officer, to GCO, to the Global Privacy Office, to the Global Compliance & Ethics or to the Amex Ethics Hotline (https://amex.ethicspoint.com/).

6.0 APPROVAL REQUIREMENTS

The Policy Custodian will facilitate the approval process, including appropriate escalation to the Privacy Risk Management Committee. For minor policy changes, Level 1 and Level 2 approval is required. For substantial changes, Level 1 through Level 4 approvals are required.

Level 1: Director, Global Colleague Privacy (GCP)

Level 2: Chief Privacy Office (CPO)

Level 3: General Counsel's Office (GCO)

Level 4: Privacy Risk Management Committee (PRMC)

7.0 EXCEPTION / CONFLICT / ESCALATION RESOLUTION

Conflicts or concerns related to Data Privacy can be directed to the Global Colleague Privacy Team at: Global Colleague Privacy

8.0 ENFORCEMENT OF ISSUED POLICIES AND PROCEDURES

The content of this policy is managed by the Global Colleague Data Privacy Team. These principles set out the Company's commitment to employees in respect of their personal data. Each company in the American Express Group that holds personal data may maintain its own additional rules and practices, which are required to be consistent with these principles and which it may modify as needed for particular products and services or to conform to local laws or customs around the world.

Noncompliance with issued policies or procedures is a breach of the terms of employment and may lead to disciplinary actions which may include termination of employment, or third-party vendor agreement.

9.0 RELATED POLICIES, PROCEDURES, REGULATORY GUIDELINES AND SUPPORTING DOCUMENTS OR LINKS

For policies and guidance supporting our enterprise wide Global Privacy framework, please visit the Privacy Information Center via The Square.

For any privacy related queries (any candidate or colleague queries within CEG or any other Business Unit) visit the Privacy Information Center to access the Contact Privacy application, which is available via Privacy Risk Assessment (PRA) application within Archer.

Important note
This document does not create a contract of employment or a contract for any specific term or condition of employment or Third Party Vendor agreement between American Express and an employee, consultant or contractor.

Additionally, the relationship between American Express and a U.S. employee is at-will, meaning that either the employee or the Company may terminate it at any time for any reason, with or without advance notice or progressive disciplinary action. The employment relationship outside the U.S. is governed by local requirements and may differ. The Company reserves the right to make changes in or discontinue company policies, compensation plans, benefits, and programs as it deems appropriate and these changes may be implemented even if they have not been communicated in this (or by change to this) document or otherwise.

If this document refers to any Company benefit program, it describes only certain highlights of the Company's benefit program.

It does not supersede the actual provisions of the applicable plan documents, which in all cases are the final authority.

Eligibility criteria and/or Company plans, programs, practices, and processes may be amended, changed, or terminated by the Company at any time without prior written notice to, or consent by, participants. This document does not constitute an obligation by the Company to maintain any particular benefit program, practice, or policy.

American Express takes reasonable efforts to ensure the accuracy of the contents of policy documents and in the administration of its policies and programs. The Company does not assume responsibility for consequential damages caused by administrative or clerical errors.

Employees should report violations of these principles to their leaders or CEG representatives, to their business unit's compliance officer, to GCO, to the Global Privacy Office, to the Global Compliance & Ethics or to the Amex Ethics Hotline (https://amex.ethicspoint.com/).

10.0 REVISION / APPROVAL HISTORY

Version #	Final Revision / Approved Date*	Revision Type: Material or Non-Material	Revision Description	CEG Policy Owner Title and Function
5	18 November 2020	Material	CEG logo, supporting links and format updates. Policy Review.	Director – Risk and Information Management
*Note – This new version supersedes all prior Final Approved/AXP Published versions				

11.0 KEY CONTACTS Employees should report violations of these principles to their leaders or CEG representatives, to their business unit's compliance officer, to GCO, to the Global Privacy Office, to the Global Compliance & Ethics or to the Amex Ethics Hotline (https://amex.ethicspoint.com/).

Any additional concerns or questions regarding data privacy may be directed to the Global Colleague Privacy team at: Global Colleague Privacy