Global Privacy Policy

Policy Area:	Regulatory Compliance	**Policy Owner:**	Richard Pooley, Chief Data Ethics and Privacy Officer
Policy Name:	Global Privacy Policy	**Policy Sponsor:**	Stephanie Parks, Chief Compliance Officer
Policy Summary:	Outlines requirements to protect Personal Data	**Effective Date:**	04/01/2020
Policy Number:	CPL.GLB.600	**Last Revision Date:**	03/31/2024

Purpose and Background

As a global provider of electronic commerce and payment solutions for merchants, financial institutions, card issuers, and consumers, Fiserv, Inc. ("Fiserv") processes Personal Data of associates, customers, consumers, and Data Subjects.

This Global Privacy Policy is based on global principles of privacy laws and the awareness that protection of Personal Data is the foundation of both sound business relationships and the reputation of Fiserv.

This Policy establishes the basis of the Global Privacy Program, which is designed to provide management and oversight of the Processing of Personal Data as follows:

- in compliance with enacted laws, regulations, and rules
- pursuant to industry best practices, where appropriate
- for privacy risk mitigation, issue tracking and resolution
- alignment with business objectives should privacy requirements guide changes to business strategy and/or product offerings

Scope

This Policy applies to all Fiserv entities and associates[1] and non-employee[2] workers. Protecting Personal Data is the responsibility of every associate and non-employee worker, who are also responsible for reading, understanding, and complying with the Policy and Program, including related policies, standards and procedures referred to within them.

[1] As used in this Policy and/or standards, "associate" means an employee of a local Fiserv employing entity. The local employing entity or its parent, Fiserv, Inc, reserves the right to alter, amend, suspend, or terminate this policyand/or standards, or their contents, at any time, at its discretion, in accordance with local laws.

[2] References to non-employee contingent workers in this Policy or any supporting standards, guidelines, or procedures, and the responsibility of these workers to comply with the terms contained in such documents, do not imply or create an employment relationship with any Fiserv company

Policy

It is the policy of Fiserv to comply with privacy laws and regulations of the countries, regions, and states where it does business.

Fiserv, under the direction of its Chief Data Ethics and Privacy Officer (CPO) has established a GlobalPrivacy Program to comply with data privacy regulations and address privacy risks. The Program scope includes:

- Governance and oversight
- Roles and responsibilities
- Policies, procedures, and standards
- Risk assessments
- Regulatory rules management
- Training and awareness
- Regulatory interactions
- Monitoring and testing
- Incident response
- Privacy notices
- Data Subject rights management
- Personal Data transfers
- Fiserv's Binding Corporate Rules (BCRs)
- Metrics and reporting

Fiserv entities may, and in some instances must, adopt their own privacy policies, standards and/or procedures based on the nature of their services or clients ("Local Policies"). Local Policies must be consistent with the Global Privacy Program as well as local laws and the Fiserv BCRs to the extent applicable and where the local entity is a member of the BCRs. The BCRs contain Data Protection Standards; Fiserv entities that sign the BCRs must follow the Data Protection Standards set forth within the BCRs.

Where there is a conflict between local law and the Policy or other Fiserv global governance documents, local law will prevail.

Where an associate on behalf of a Fiserv entity believes a conflict with applicable laws prevents the entity from fulfilling its duties under this Policy or the BCRs, (including following the advice of an applicable Data Protection Authority), the associate must notify the Data Protection Officer (DPO) and the CPO who will (in consultation with Legal and the relevant Data Protection Authority, where necessary) decide the appropriate response to the perceived conflict.

Governance and Oversight

The Global Privacy Policy is part of a comprehensive Global Privacy Program that encompasses strategic, tactical and operational coverage of privacy matters. The Program is managed by the CPO.

Each line of business is responsible for compliance with the Privacy Program including assisting the Global Privacy Office with implementing policies and procedures, managing privacy-related issues, building a culture of privacy awareness, and communicating with key stakeholders on privacy-related issues.

The Chief Information Security Officer (CISO) and the DPO, along with Legal and Global Cyber Security Services (GCSS), shall work collaboratively with the CPO to establish the programs, protocols, and tools necessary to meet the objectives of the Policy.

Escalation

For questions regarding the Policy or Global Privacy Program, contact the CPO at dpo@fiserv.com.

Enforcement

Failure to comply with this Policy may lead to disciplinary action up to and including termination of employment for associates and/or pursuit of legal remedies.

Exceptions

There are no exceptions to this Policy unless permitted by law and approved through the Regulatory Compliance exception process. Exceptions must be sought by contacting the Policy Owner named in the header of this Policy, who will initiate the exception process for Regulatory Compliance.

Related Documents

Privacy program documents, standards, and relevant documentation are available on FUEL on the Global Privacy Office page.

Fiserv's Data Ethics Framework, associated program and other relevant documentation (including Guidelines for Responsible Artificial Intelligence and Machine Learning) are available on FUEL on the Data Ethics page.

Definitions

"Binding Corporate Rules (BCRs)": BCRs are legally binding intra-group agreements that govern the cross-border transfer of Personal Data from within the European Economic Area (EEA) to a country outside of the EEA in compliance with applicable laws.

"Data Subject": An identified or identifiable natural person; an identifiable natural person is a

living individual 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.

"Fiserv Entities**":** Fiserv, Inc. and its subsidiaries, (and may include joint ventures, strategic alliances, and/or affiliates, depending on the content of the policy).

"Personal Data**":** Any information relating to a Data Subject, irrespective of the information by itself being enough to identify a particular person. Personal Data can relate to anyone whose information Fiserv obtains in connection with its business activities or the services it provides, including Fiserv associates and customers (and employees) of Fiserv clients.

"Processing": Any operation which is performed on or using Personal Data, including but not limited to collection, access, display, recording, storage, transfer, alteration, disposal, and disclosure.

Roles and Responsibilities

The CPO is responsible for defining and implementing the Global Privacy Program designed to comply with data privacy regulations as defined in the Policy section of this document, to address privacy risks, and to monitor for areas of developing risk (such as the expansion of the use of high-risk technologies like Artificial Intelligence/Machine Learning).

It is the collective responsibility of the CPO, the CISO, any relevant DPO, the Legal Department, and GCSS to establish the standards and implement activities that meet global privacy mandates as amended from time to time.

It is the responsibility of associates to complete Privacy training, abide by the Fiserv Privacy Principles (included in the Fiserv Global Privacy Program document), abide by local privacy mandates and report any perceived conflict with applicable laws to the CPO or local DPO where applicable. It is the responsibility of the local DPO to communicate such reports to the CPO.

It is the responsibility of the CPO to consult with the Legal Department and the relevant Data Protection Authority, where necessary, to decide the appropriate response to the perceived conflict.

Training and Awareness

Privacy training is required for all new associates, and refresher training is required for current associates on an annual basis. In addition, contractors and non-employee workers may be required to complete such training as is required to perform services for Fiserv.

Fiserv will post a copy of the BCRs Data Protection Standards on its internal and public websites. In addition, a copy of the BCRs Data Protection Standards will be sent to Data Subjects upon request.

The Global Privacy Office, in collaboration with GCSS, oversees and manages a Data Protection Awareness Program to publish privacy and security awareness reminder materials on a regular basis.

Contact Information

For additional information, please contact the Global Data Privacy Office at dpo@fiserv.com.

Revision History

Policy Approver	Stephanie Parks, Chief Compliance Officer
Revision Date	March 31, 2024
Next Renewal Date	April, 2025
Approval Cycle	Annual