ACI Worldwide
Real-Time Payments

DATA PRIVACY & PROTECTION POLICY

REVISION DATE – MARCH 12, 2024
LAST REVIEWED DATE – MARCH 12, 2024

TABLE OF CONTENTS

INTRODUCTION 3

POLICY SUMMARY 3

DEFINITIONS 3

ROLES AND RESPONSIBILITIES 4

LAWFUL PROCESSING OF PERSONAL DATA 4

LIMITATION OF PURPOSE FOR PROCESSING PERSONAL DATA 5

PERSONAL DATA MINIMIZATION 5

PERSONAL DATA ACCURACY 5

LIMITATION ON STORAGE 6

SECURITY OF PERSONAL DATA 6

INTERNATIONAL TRANSFERS OF PERSONAL DATA 6

RECORD OF PERSONAL DATA PROCESSING 6

THIRD PARTY PROCESSING OF PERSONAL DATA 7

DATA SUBJECT RIGHTS 7

DATA PRIVACY AND PROTECTION ISSUE MANAGEMENT 7

POLICY GOVERNANCE 7

POLICY COMPLIANCE 7

POLICY EXCEPTIONS 7

CONTACT 7

DOCUMENT INFORMATION 7

APPENDIX 9

INTRODUCTION

This Policy sets forth the requirements for how Personal Data are to be handled and processed in the course of ACI's business operations. This Policy is to be implemented in coordination with those policies referenced herein and identified below under "Related Documents".

ACI is committed to safeguarding the data privacy rights and privileges of Data Subjects as part of its ongoing responsibility to comply with Applicable Laws and meet its ethical and social responsibilities to the public.

This policy is approved by the Risk and Compliance Steering Committee, provided to the ACI Board, and applies to ACI Worldwide, Inc. and its subsidiaries (ACI) and all employees, temporary staff, contractors, contingent workers, and consultants globally.

POLICY SUMMARY

ACI commits to adhere to established Data Privacy Principles. All processing of Personal Data by ACI in the course of its operations shall be conducted in a manner which observes and respects the following Data Privacy Principles:

- Lawfulness of Personal Data Processing – ACI shall process Personal Data in a lawful, fair, and transparent manner.
- Limitation of Purpose – ACI shall process Personal Data for specified, explicit and legitimate purposes and will not process that Personal Data for any other reasons not compatible with those purposes.
- Personal Data Minimization – ACI shall collect only Personal Data which is adequate, relevant, and limited to what is necessary to fulfil the purposes for collection.
- Personal Data Accuracy – ACI shall keep Personal Data accurate and, where necessary, kept up to date, and where Personal Data is inaccurate, shall take every reasonable step to ensure it is corrected or erased without delay when appropriate to the purpose for Processing.
- Limitation on Storage – ACI shall keep Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed.
- Security of Personal Data – ACI shall process Personal Data in a manner that ensures the appropriate security of it, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or operational measures.

DEFINITIONS

For purposes of this Policy, the following definitions apply:

Applicable Law - Laws, regulations, or industry standards which govern ACI's collection, use, storage, processing, and disclosure of Personal Data.

Data Controller – A 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. The term shall be inclusive of equivalent terms under Applicable Law.

Data Subject- A natural or legal person to whom Personal Data refers as specified under applicable Law. The term shall be inclusive of equivalent terms under Applicable law.

Personal Data – Any information which identifies or is capable of being used to identify a Data Subject, but shall have the meaning prescribed under Applicable Law. As used in this Policy, the term "Personal Data" shall be synonymous with, and inclusive of, the terms Personal Information, Protected Health Information ("PHI"), Sensitive Consumer Financial Information ("SCFI"), or Non-Public Personal Information as those terms are defined by Applicable Law. All general references to Personal Data in this Policy shall be inclusive of Special Categories of Personal Data. Examples of Personal Data include, but are not limited to, a Data Subject's name, address, email address, Social Security or similar government ID number, internet protocol ("IP") address, and financial account numbers.

Processing- 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.

Data Processor- A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller. The term "Data Processor" shall be inclusive of equivalent terms under Applicable Law, including "Operator", "Entrusted Party", "Processor", "Data Intermediary", "Data Custodian", and "Service Provider."

Sensitive Personal Data - Personal Data that reveals a Data Subject's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union memberships

ROLES AND RESPONSIBILITIES

All roles and responsibilities defined in the Enterprise Risk Management Policy and Compliance Risk Management Policy shall have the same meaning in this Policy. The roles and responsibilities listed below are in addition to those roles and responsibilities.

Data Protection Officer: Monitors, informs, and advises on data protection obligations as required by various countries.

Leaders of Second Line of Defense Functions (ERM, Compliance, Global Information Security): Executing strategic Data Protection-related objectives across ACI.

Business Unit: Responsible for processing of personal data, which may include employees and/or data subjects of customers and other third parties.

LAWFUL PROCESSING OF PERSONAL DATA

ACI's processing of Personal Data shall be conducted on a lawful basis under Applicable Law, which may consist of one or more of the following lawful bases:

- The Data Subject has provided their consent for the processing of their Personal Data as prescribed by Applicable Law.
- The Data Subject has provided their explicit consent for the processing of their Personal Data which is also Sensitive Personal Data as prescribed by Applicable Law.
- The Personal Data is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract.

- The processing of Personal Data is necessary for compliance with a legal obligation to which ACI is subject.

- The processing of Personal Data is necessary to protect the vital interests of the data subject or of another natural person.

- The processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in ACI or an ACI customer where ACI is serving as a Data Processor.

- The processing of Personal Data is in the "legitimate interests" of ACI and where those "legitimate interests" are not overridden by the interests or fundamental rights and freedoms of Data Subjects.

LIMITATION OF PURPOSE FOR PROCESSING PERSONAL DATA

ACI shall only process Personal Data for those purposes which are transparently notified to Data Subjects as prescribed by Applicable Law or which are reasonably related to or compatible with those purposes. ACI shall consider the following factors when determining whether the processing of Personal Data is reasonably related to or compatible with the purposes notified to Data Subjects:

- Any link between the purposes for which the Personal Data have been collected and the purposes of the intended further processing

- The context in which the Personal Data have been collected, in particular regarding the relationship between the Data Subject and ACI

- The nature of the Personal Data, in particular whether Sensitive Personal Data are processed or whether Personal Data related to criminal convictions and offences are processed

- The possible consequences of the intended further processing for the Data Subject

- The existence of appropriate safeguards, which may include encryption or pseudonymization

ACI shall not process Personal Data for any new purposes or additional purposes not related to or compatible with the original purpose for collection without notifying Data Subjects of those purposes as required under Applicable Law.

PERSONAL DATA MINIMIZATION

ACI will process only that Personal Data which is appropriate, relevant and limited to the minimum necessary to fulfil the purpose for its collection, both quantitatively and qualitatively. Each department responsible for the processing of Personal Data shall evaluate and document what Personal Data is necessary for the processing, including whether anonymized data can fulfil the purpose for that processing.

PERSONAL DATA ACCURACY

ACI will ensure that Personal Data processed under its control or direction is accurate and up-to-date as necessary to fulfill the purposes for processing. Appropriate procedures shall be adopted to ensure that Personal Data are deleted, corrected, supplemented, or updated as necessary under Applicable Law.

LIMITATION ON STORAGE

ACI will not store Personal Data any longer than is necessary to fulfill the purposes for its processing, including to comply with ACI's legal obligations. Personal Data deemed to no longer be necessary for ACI's processing or compliance with legal obligations shall be deleted or anonymized as soon as possible and consistent with ACI's *Record Retention Policy*.

It is the responsibility of each Business Unit processing Personal Data to implement appropriate procedures for the deletion or anonymization of Personal Data which are no longer needed.

SECURITY OF PERSONAL DATA

ACI shall protect all Personal Data from unauthorized access, loss, alteration, or deletion using appropriate technical and organizational measures, taking into account technological developments, the cost of implementation, organizational changes, emerging threats, the nature, scope, and purpose for the processing of Personal Data, and the risks of harm to the rights and freedoms of the Data Subjects whose Personal Data are being processed.

ACI Global Information Security shall be responsible for the oversight and governance of technical and organizational security measures for the protection of Personal Data. Such measures are to be documented in ACI's Information Security Policies developed and maintained by ACI Global Information Security.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

ACI shall conduct cross-border transfers of Personal Data in accordance with the requirements of Applicable Law. Acceptable mechanisms for the transfer of Personal Data under Applicable Law, include:

- An adequacy determination by relevant authorities
- Appropriate Safeguards such as: (i) Standard Contractual Clauses issued by relevant authorities; (ii) Binding Corporate Rules approved by relevant authorities; (iii) a Code of Conduct approved by relevant authorities; or (iv) a Certification Mechanism approved by relevant authorities
- Derogations for specific situations, such as data subject's explicit consent, having been informed of the possible risks of such transfers in the absence of an adequacy determination or other appropriate safeguards
- The prior approval of relevant authorities where no other mechanism for cross-border transfer is available

Where there is no adequacy determination in place from relevant authorities, ACI shall conduct a data transfer impact analysis to determine whether the mechanism for transfer adequately protects the rights and freedoms of data subjects from the laws of the importing country, in particular from any type of mass warrantless government surveillance requests.

RECORD OF PERSONAL DATA PROCESSING

ACI shall document all processing of Personal Data, including that processing being conducted by third parties on behalf of ACI. Each department responsible for the processing of Personal Data shall maintain a record of their processing activities in the manner prescribed to them by Enterprise Risk Management & Compliance.

THIRD PARTY PROCESSING OF PERSONAL DATA

ACI shall engage only those third parties who are able to provide sufficient guarantees of compliance with the requirements of Applicable Law and in accordance with the ACI Third Party *Risk Management Policy*.

ACI will contractually obligate all third parties to whom it discloses Personal Data for further processing to process and protect that Personal Data in accordance only with ACI's instructions and Applicable Law.

DATA SUBJECT RIGHTS

ACI shall honor the rights and freedoms granted to Data Subjects with regard to their Personal Data as prescribed by Applicable Law and in accordance with its Data Subject Rights Procedures.

DATA PRIVACY AND PROTECTION ISSUE MANAGEMENT

Any operational risk issue that involves data privacy and protection shall follow the "Issue Management & Loss Events" section of the *Enterprise Risk Management Policy*.

POLICY GOVERNANCE

This Policy is required to be reviewed and approved minimally on an annual basis by the Policy owner and domain approvers. The Policy owner is responsible for conducting the review and necessary revisions as well as collecting the required approvers for their business unit. The Policy owner reserves the right to modify this policy and all procedures associated with this policy, in its sole discretion, at any time.

POLICY COMPLIANCE

Failure to adhere to or willful disregard of any standards or requirements set forth in this Policy can be grounds for disciplinary action up to and including termination of employment or contract with ACI Worldwide, Inc.

POLICY EXCEPTIONS

Exceptions to this Policy may only be authorized by the Head of Enterprise Risk Management & Compliance (or his/her designees). All requests for exceptions to this Policy must be documented with the reasons for the exceptions clearly identified in accordance with the corporatewide compliance policies and procedures governance process.

CONTACT

Any questions regarding interpretation of this Policy should be directed to Enterprise Risk Management & Compliance by emailing *mbox-ACI-Privacy-DataProtection@aciworldwide.com*.

DOCUMENT INFORMATION

Policy Owner: Dan O'Brien

Policy ID: ACIW-047

Related Documents:

This policy is subordinate to the *Enterprise Risk Management Policy*.

Related policies and documents include, but are not limited to:

- ACI Privacy Statement – Publicly-available statement to reflect how ACI Worldwide handles personal data and any legal disclosures required under consumer-protection law.

- ACI Payments, Inc. Privacy Statement -- Publicly-available statement to reflect how ACI Payments, Inc., handles personal data and any legal disclosures required under consumer-protection law.

- ACI Record Retention Policy - Establishes the record retention period based on type of records and legal or compliance guidelines that dictate the length of time and disposal.

- ACI Information Security Policy - Defines rules and processes that protect company information resources.

- ACI Third Party Risk Management Policy -– Provides guidance around risk identification, measurement, management, and reporting for third parties that provide products and services.

- ACI Data Subject Rights Procedures - Lists procedures that data subject rights are privy to under European Union laws.

- Data Privacy Impact Assessment – Maps the projected impacts involving the processing of personal data on the rights of individuals.

- ACI Incident Management Response – *Response guidance around data breaches.*

APPENDIX

ACI complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. ACI has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF,. ACI has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland.

The EU-U.S. DPF Principles and Swiss-U.S. DPF Principles are:

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability

Further information regarding the EU-U.S. DPF Principles and Swiss-U.S. DPF Principles can be found at: *https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles*.

If there is any conflict between the terms in this Notice and the EU-U.S. DPF Principles and/or the Swiss/U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov.

ACI is responsible for the processing of the Personal Data it receives, under the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF, and subsequently transfers to a third party acting as an agent on its behalf. ACI complies with the EU-U.S. DPF and Swiss-U.S. DPF Principles for all onward transfers of Personal Data from the EU, UK and Switzerland, including the onward transfer liability provisions.

The Federal Trade Commission has jurisdiction over ACI's compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF. In certain situations, ACI may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Questions or concerns regarding this Policy may be directed to the Policy Owner, the DataProtection Officer, at *mbox-aci-privacy-dataprotection@aciworldwide.com.*