ACI DATA PROTECTION POLICY

CLASSIFICATION: ACI WORLDWIDE CONFIDENTIAL

Last Updated Date – January 18, 2019
Last Reviewed Date – January 29, 2020

Policy ID: ACIW-047
Policy Owner Contact Info:
Brad Mullman, Chief Compliance Officer
brad.mullman@aciworldwide.com
(239)403-4632

ANY PAYMENT,
EVERY POSSIBILITY.®

Table of contents

PURPOSE

This Global Data Protection Policy ("Policy") describes how ACI Worldwide, Inc. and its affiliates and subsidiaries, Official Payments Corporation and Retail Decisions, Inc. (collectively, "ACI"), undertake activities regarding the collection, use, processing, and transfer of "Personal Data" (as defined in Section 2 of this Policy) throughout the world.

SCOPE

ACI is committed to complying with the applicable data privacy and security requirements in the countries in which it operates. This Policy describes the manner by which ACI collects, uses, processes, and otherwise transfers certain Personal Data (as defined and described in more detail below) in connection with the employment relationship. This Policy applies to certain Personal Data about employees, officers, directors, contractors, and agents of ACI.

DEFINITIONS

For purposes of this Policy, capitalized terms not otherwise defined within the body of this Policy, shall have the following meanings:

"**Data Subject**" means the person to which data refers. Data Subjects include employees, officers, directors, contractors and agents.

"**EU Personal Data**" means Personal Data about a Data Subject located in the EU that is collected or processed by an entity established in a European Union Member State, or that was processed on equipment located in a European Union Member State.

"**Personal Data**" means personally identifiable information related to a Data Subject that is unique to that Data Subject and who can be identified from that data; and includes Sensitive Data. Categories of Personal Data that may be collected and processed by ACI are set forth in Sections 3.1.1 through 3.1.3 of this Policy.

"**Sensitive Data**" means Personal Data containing information as to the Data Subject's:

- Race or ethnic origin;
- Religious beliefs or other beliefs of a similar nature;
- Political opinions;
- Physical or mental health or condition;
- Sexual history or orientation;
- Trade union membership; or

Commission or alleged commission of any offense and any related court proceedings.

POLICY CONTENT

Data Collection and Processing

ACI may collect and process the following categories of Personal Data:

1. **Personal and family information,** including name and contact information (home address, telephone and fax numbers and email address and additional emergency contact information), gender, marital status and information about dependents, date of birth, nationality and residency information, social security or national insurance number or other local equivalent, and bank account or credit card details; and

2. **Employment related information,** including job/position title, supervisor name and title, work contact information (building location and address, telephone and fax numbers and email address), badge number, territory, employee ID, region, information security data (e.g., username, password(s),

access control data and similar security and technical information), division, subdivision, department, employment contract information, professional certifications, information regarding expatriated status, working time and leave entitlements, salary and related compensation data (bonus information, pay scale area and type and any salary-related changes), stock option and pension plan participation information, benefits and perquisites information, company property on loan, allowance information (housing, vehicle, transportation, meal, family or other), information regarding previous work experience (including references from previous employers), qualifications and work history, skills assessment levels, educational background, performance-related information, awards, hire date, seniority date, departure date (where applicable), reports from executive search or employment firms (where applicable), and any additional information contained in manager financial conflict of interest certification statements (as further described in such statements and where applicable).

3. **Other data,** including data obtained from ACI's closed circuit television systems may capture employees on video in the course of ordinary business. Cameras are only setup in common facility entrance points to help ensure employee safety, or to cover strategic technology assets, as required by the Company's contractual obligations and industry requirements. Cameras are never to be positioned to monitor individual employee behavior.

ACI also may collect and process certain information regarding a Data Subject's spouse, family members, or other dependents for emergency contact and benefits administration purposes. ACI will not collect or process any Personal Data, and particularly Sensitive Personal Data, that is prohibited by local law. The type of Personal Data actually collected by ACI or an affiliate/subsidiary may vary from jurisdiction to jurisdiction, and some jurisdictions may not collect all of the categories of Personal Data listed above.

ACI collects, uses, and otherwise processes Personal Data for the following purposes: payroll, employee related services and benefits, employee safety/physical security, and medical and health insurance related purposes.

ACI may collect and process the following categories of Sensitive Data as allowed by applicable law: race for reporting purposes; and physical or mental health or condition for the purposes of determining and processing short and long term disability benefits.

If employees do not provide the Personal Data that ACI requires for the purposes described above, then ACI may not be able to fully provide such employees with certain employment-related services or benefits.

Only a limited number of restricted individuals within ACI's human resources, finance, legal, insurance, physical security, and IT departments, as well as certain managers, will receive access to Personal Data, and only when necessary in connection with their job responsibilities.

ACI will retain Personal Data no longer than is necessary to carry out the purposes listed in this Policy, or as required by applicable law.

ACI does not collect, use, disclose, or otherwise process Personal Data for direct marketing purposes.

Transfers of Data Internally

1. As a global organization, personal data collected within the scope of this policy may be shared globally throughout ACI's organization. If your personal information is transferred to an ACI recipient in a country that does not provide an adequate level of protection for personal information, ACI will take measures designed to ensure that your personal information is adequately protected.

2. Any transfer of EU Personal Data shall be pursuant to a contract embodying the EU Commission's Model Contractual Clauses.

Transfer of Data to Third Parties

1. As part of its normal business operations, ACI may disclose Personal Data to third party service providers in connection with human resources, employee safety/physical security, payroll or benefits related tasks, and information technology support.

2. Personal Data will not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.

3. Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the Personal Data was originally collected or other purposes authorized by law.

4. All transfers of Personal Data to third party data processors for further processing will be subject to written agreements.

5. EU Personal Data shall not be transferred to a third party in a country or territory outside the European Economic Area unless the transfer is made to a country or territory recognized by the EU as having an adequate level of legal protection or is made in compliance with one of the mechanisms recognized by the EU as providing adequate protection when transfers are made to countries or territories lacking an adequate level of data protection, or as otherwise allowed by applicable law.

6. ACI may also disclose Personal Data to governmental agencies and regulators, social organizations, external advisors, courts and other tribunals, and government authorities, to the extent required or permitted by applicable legal obligations.

Choice

1. For information about an employee collected in the EU/EEA or as otherwise required by law, employees may request to exercise some or all the following choices regarding how their personal information is processed.

    - Withdraw consent: They may request to withdraw the consent they have previously provided for the processing of their personal information.
    - Erasure of personal information - They may request to erase or delete all or some of their personal information.
    - Change or correct personal information: They may request edit to some of their personal information.
    - Object to, or limit or restrict use of personal information: They may request to stop using all or some of their personal information.
    - Right to access and/or take their data: They may also request to obtain a copy of some or all of their personal information in machine readable form.

To exercise these choices, please complete the following request form, or contact your local HR representative directly. If a request cannot be satisfied, adequate explanation as to why will be included as part of the response to the employee.

Data Security

ACI maintains appropriate and reasonable physical, technical and organizational measures to ensure the security of Personal Data, including the prevention of the alteration, loss, damage, unauthorized processing or access to Personal Data, having regard to the state of the art, the nature of the Personal Data, and the risks to which it is exposed by virtue of human action or the physical or natural environment. ACI also maintains

reasonable procedures to help ensure that such data is reliable for its intended use, accurate, complete and current.

POLICY COMPLIANCE

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

POLICY EXCEPTIONS

Exceptions to this policy must be requested and approved in Archer. Depending on the type of exception requested, required approvers may include the requestor's leadership team, Global Information Security, Corporate Compliance, Business Process Owner and Product Development Leadership.

REVIEW OF POLICY AND PROCEDURES

This Policy is required to be reviewed and approved minimally on an annual basis by the Policy owner and domain approvers. ACI Worldwide reserves the right to modify this policy and all procedures associated with this policy, in its sole discretion, at any time.

RELATED DOCUMENTS

ACI Privacy Statement - *https://www.aciworldwide.com/privacy-policy*

APPENDIX

ACI, and its respective subsidiaries covered by this policy (Official Payments Corporation and Retail Decisions, Inc.), complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. ACI has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

ACI is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on ACI's behalf. ACI complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, ACI is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. 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 (refer to "Disclosure to Third Parties" in Section 5 for more details).

In compliance with the Privacy Shield Principles, ACI commits to resolve complaints about its collection or use of your Personal Data. EU or Swiss individuals with inquiries or complaints regarding this Policy or the Privacy Shield Principles should first contact ACI at:

ACI Worldwide Corp.

Attention: Chief Privacy Officer

6060 Coventry Drive Elkhorn, NE 68022 U.S.A.

Email: mbox-aci-privacy-dataprotection@aciworldwide.com

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedbackform.truste.com/watchdog/request. Under certain conditions, more fully described on the Privacy Shield website at https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

ACI has further committed to cooperate with EU and Swiss data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU or Switzerland in the context of the employment relationship.

Questions or concerns regarding this Policy also may be directed to the Policy Owner, or ACI's Data Protection Officer at Brad.Mullman@aciworldwide.com