EPAY Systems Client Data Retention Policy

Table of contents

Version 1.3

Purpose and Scope

EPAY Systems is committed to protecting our systems, information, and our clients' information. The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by EPAY Systems, and their clients are discarded at the proper time and in accordance with applicable biometric and data privacy laws. This policy defines the retention requirements for customer data in the EPAY Systems Blueforce SaaS service. This policy applies to all EPAY Systems employees or contractors working on behalf of EPAY Systems.

EPAY Systems business systems include:

- Client TLM Data/Storage (non-biometric)
- Biometric Client Data (facial/fingerprint biometrics)

Reference Documents

- EPAY Systems IT Security Policy

Policy

EPAY Systems will define a retention schedule for all systems and data in use within the organization and will document them in the Data Retention Schedule.

Data retention schedule for customer data – SaaS Services

The EPAY Systems Service Agreement specifies that customer data will be available in industry-standard format for download upon termination or completion of the service (free of charge) and will have 90 days to request/receive such data before it is archived and taken offline. Except as otherwise agreed or required by applicable law, EPAY Systems will retain **non-biometric data** for 7 years upon termination.

BIOMETRIC DATA RETENTION SCHEDULE

- EPAY Client's Employee biometric data contained on EPAY Servers is removed within 5 business days of contract termination date in compliance with BIPA (Biometric Information Privacy Act).
- Employee biometric data contained on Walter Biometric Devices (Time Clocks) and server database is removed immediately upon an employees' termination (i.e., an employee is made inactive in the system) in compliance with BIPA (Biometric Information Privacy Act).

Responsibilities

Employees and Contractors

All employees who create and use records and information are responsible for maintaining EPAY Systems Records according to this Policy.

Management and Business Units

All levels of management within EPAY Systems are responsible for ensuring compliance with this Policy within their respective group, region, or function.
They are responsible for ensuring that their employees know where to locate the current Data Retention Schedule and that hard copy and electronic files are kept, stored, or destroyed in compliance with this Policy.

Retention Requirements

- EPAY Systems will retain or destroy data files in compliance with the retention periods stated in the Data Retention Schedule.
- The retention periods provided in the Data Retention Schedule are intended to be as long as possible to make the historical records available for any legal, contractual, and/or operational requirements. Records will be kept only for the period stated in the Schedule and will be destroyed or discarded at the stated retention period expiration.

Safeguarding of Data

Measures will be taken to ensure that the information can be accessed by authorized users during the retention period and will also be stored according to its classification level. For EPAY Systems internal systems, the responsibility for the storage belongs to IT/MIS team.

Disposal of Data

As data expires according to the Retention Schedule, the data will be deleted, shredded or otherwise destroyed in accordance to its classification and destruction requirements. Overall responsibility for the disposal of data belongs to the IT/MIS team.

Policy Enforcement

The EPAY Systems Chief Information Security Officer (CISO) is responsible for ensuring compliance with this policy and will assist with the protection of EPAY Systems data. Any employee found to willfully or intentionally violate this policy may be subject to disciplinary action, up to and including termination of employment.