Papaya Insurtech Data Deletion Policy

Introduction

This document provides an overview of the data deletion process in the system. There are two types of data deletion: soft deletion and hard deletion. Soft deletion is performed first, and if the customer requests it, hard deletion can be performed.

Soft Deletion Data

Stage 1 - Deletion Request

The deletion of Customer Data begins when the customer initiates a deletion request. Generally, a deletion request is directed to a specific resource, Policy/Claim/Claim Document. Deletion requests may be handled in different ways depending on the scope of the customer's request:

- Resource Deletion: Individual resources containing Customer Data, such as claim documents, can be deleted in a number of ways from the Care Portal or via API. For example, Customers may issue a remove of claim document or make a DELETE API request command to delete a document through the API or customers may select a file and delete it from the Insurer Portal.
- Account Deletion: Customers can request to deactivate the accounts. Deactivated accounts cannot log in or perform any action in the system. Deactivated accounts can be reactivated later. Customers can also request to delete the accounts, which will delete all the data associated with the account.

While deletion requests are designed primarily to be used by Customers to manage their data, Papaya may issue deletion requests automatically, for instance when a customer terminates their relationship with Papaya.

Stage 2 - Soft Deletion

Soft deletion is the natural point in the process to provide a brief internal staging and recovery period to ensure that there is time to recover any data that has been marked for deletion by accident or error. The data remains in the system until the customer requests hard deletion. Audit logs are maintained for all deletion actions.

Hard Deletion Data

Stage 3 - Logical Deletion from Active System

After the data is marked for deletion and any recovery period has expired, the data is deleted successively from Papaya's active and backup storage systems. On active systems, data is deleted in two ways.

For all types of Customer Data except Claim Documents, copies of the deleted data are marked as available storage and overwritten over time. In an active storage system, deleted data is stored as entries within a massive structured table. Compacting existing tables to overwrite deleted data can be expensive, as it requires re-writing tables of existing (non-deleted) data, so mark-and-sweep garbage collection and major compaction events are scheduled to occur at regular intervals to reclaim storage space and overwrite deleted data.

For Claim Documents, Customer Data is also deleted through cryptographic erasure. This is an industry standard technique that renders data unreadable by deleting the encryption keys needed to decrypt that data. One advantage of using cryptographic erasure, that logical deletion can be completed even before all deleted blocks of that data are overwritten in Papaya System's active and backup storage systems.

Stage 4 - Expiration from Backup System

Similar to deletion from Papaya's active systems, deleted data is eliminated from backup systems using both overwriting and cryptographic techniques. In the case of backup systems, however, Customer Data is typically stored within large aggregate snapshots of active systems that are retained for static periods of time to ensure business continuity in the event of a disaster (e.g., an outage affecting an entire data center), when the time and expense of restoring a system entirely from backup systems may become necessary. Consistent with reasonable business continuity practices, full and incremental snapshots of active systems are made on a daily, weekly, and monthly cycles and retired after a predefined period of time to make room for the newest snapshots.

When a backup is retired, it is marked as available space and overwritten as new daily / weekly / monthly backups are performed.

Note that any reasonable backup cycle imposes a pre-defined delay in propagating a data deletion request through backup systems. When Customer Data is deleted from active systems, it is no longer copied into backup systems. Backups performed prior to deletion are expired regularly based on the pre-defined backup cycle.

Finally, cryptographic erasure of the deleted data may occur before the backup containing Customer Data has expired. Without the encryption key used to encrypt specific Customer Data, the Customer Data will be unrecoverable even during its remaining lifespan on Papaya's backup systems.

Cloud Provider Data Deletion

The Papaya System is hosted on AWS Cloud. For more information on data protection and compliance on AWS, refer to the following documentation:

- Data protection in Amazon EC2
- Data protection in Amazon S3
- Navigating GDPR Compliance on AWS