



Data Storage, Erasure & Retention Policy

Title: Data Storage, Erasure & Retention Policy

Effective Date: October 2025

Review Date: October 2026

Process Owner: Compliance

Approved by: Head of Global Risk, Compliance & Safety



Contents

1	About this document	3
1.1	Document history	3
1.2	Contributors	3
1.3	Reviewers	3
2	Introduction	3
2.1	Purpose and scope	3
2.2	Roles and responsibilities	4
2.3	Reviews	4
3	Data Retention Principles.....	5
4	Storage & Security	5
5	Retention Periods.....	6
6	Deletion.....	7
7	Policy Violations	7



1 About this document

1.1 Document history

Date	Version	Release Notes	Author
7 October 2025	1.0.		Bree Bakaric

1.2 Contributors

Name	Role
Bree Bakaric	Senior Data Privacy & Compliance Associate

1.3 Reviewers

Name	Role
Bree Bakaric	Senior Data Privacy & Compliance Associate
Selby Marshall	Head of Global Risk, Safety & Compliance

2 Introduction

2.1 Purpose and scope

The purpose of this Policy is to outline JOE & THE JUICE's approach to data storage, erasure & retention practices. Whilst all personal & non-personal data held by JOE & THE JUICE should be retained only for as long as is necessary from a business & regulatory standpoint, this policy is specific to the retention of personal data, which is any information that can directly or indirectly identify a person, including **but not limited to** personal details, contact information, health & employment records, financial records, biometric & genetic data, religious & political beliefs.

This policy outlines the controls & procedures JOE & THE JUICE has implemented to manage the retention & deletion of customer, employee & third-party personal data.

Data retention refers to the storage of data for a specific period of time, typically for legal, regulatory, business or operational purposes. Data retention involves determining how long various types of data should be retained before being deleted, guided by business needs & ensuring compliance with relevant laws & regulations.



2.2 Roles and responsibilities

Implementing & adhering to organisational policies & procedures is a collaborative effort requiring a commitment from all personnel, including management, internal employees & users of system components, along with vendors, contractors & other relevant third parties.

Each department is responsible, in collaboration with IT, for ensuring that the data they collect, process & store is necessary for the purpose for which it is collected & is deleted in accordance with the retention periods set by each department.

In summary, department responsibilities can be categorised as follows:

Responsible	Responsibilities
• Joe & The Juice Compliance Team	• Control and compliance with policy • Yearly review & Policy Approval • Management of retention period registry
• Joe & The Juice IT Team	• Supporting ability to deliver retention periods in software systems
• Joe & The Juice Employees & System Owners	• Ensuring retention periods are adhered to

If you become aware that certain personal data has not been deleted in accordance with your department's retention periods, you must make your manager or the Compliance team aware of this to ensure that the data is deleted.

2.3 Reviews

This document shall enter into force, unless otherwise indicated on the day of its approval and shall remain valid until it is modified or revoked in a subsequent document.

This document may be repealed in whole or in part by the competent area that approved it and in a subsequent document that expressly so states in a repealing provision.

JOE & THE JUICE will re-evaluate and update this Policy in accordance with applicable data privacy laws & regulations in each jurisdiction that it operates.

This document will be reviewed at least once a year.



3 Data Retention Principles

JOE & THE JUICE is committed to the following principles when storing personal & non-personal data:

- Compliance with applicable laws & regulations, including privacy, employment & tax laws & regulations.
- Security & respect for employees', customers', job applicants & business partners' company & personal data.
- Openness and transparency in how we determine appropriate retention periods & how we store data.
- Accountability for balancing the business' needs in storing personal data for operational purposes against the risks associated with said storage.

JOE & THE JUICE strives to ensure that personal data we collect is only stored for:

- 1) as long as is necessary to achieve the business purpose for which it is collected; and/or
- 2) as long as is required under relevant legislation.

4 Storage & Security

Where possible, data is to be stored in an anonymised or pseudonymised format.

Technical and organisational security measures must be implemented by each department to ensure the confidentiality & security of personal data. Examples of security measures include, but are not limited to:

Technical Security Measures

- Role-based access restrictions
- Multi-factor authentication
- Anonymisation
- Pseudonymisation
- Data encryption
- Secure VPNs for remote access
- Password management policy
- Incident reporting procedure
- Data back-up



Organisational Security Measures

- Periodic reviews & audits
- Secure storage of hard-copy data
- Disaster recovery plans
- Secure disposal of data
- Segmented access control
- Data Processing Agreements for all software vendors/processors
- Acceptable Use Policies

5 Retention Periods

Retention periods are to be set by each team in accordance with the principles of data minimisation in accordance with relevant privacy legislation, including but not limited to the *General Data Protection Regulation* (GDPR), *California Consumer Privacy Act* (CCPA), *California Privacy Rights Act* (CPRA), *United Kingdom General Data Protection Regulation & Data Protection Act*.

Data minimisation requires that organisations:

- (a) Collect only the personal data that is strictly necessary to fulfil the purpose for which it is collected.
- (b) Limit access to data collected to only those within the organisation that require the information.
- (c) Avoid storing data for longer than is required for the purpose.
- (d) Regularly review data collected & retained to ensure it remains relevant & necessary to keep.

Retention periods should also be compliant with the minimum record storage requirements under other legislation applicable to employment, financial & tax records in each jurisdiction that we operate.

Each team should liaise with the Compliance team to set appropriate retention periods for personal data they store, in accordance with relevant legislation & the principles of data minimisation.

Compliance shall keep a register of agreed retention periods, linked [here](#). Any changes to this register must first be agreed with Compliance.



6 Deletion

Before disposal or reuse of equipment, JOE & THE JUICE IT will verify that all equipment containing storage media has been purged of any personal data and licensed software. This data will either be securely overwritten or entirely removed.

All physical records held by JOE & THE JUICE which contain personal data will be shielded from loss, destruction, falsification & unauthorised access through the implementation of security measures by each department responsible for maintaining those records.

In collaboration with IT, each department must ensure that deletion of personal data it has stored is in accordance with the retention periods set by each department. The erasure of this data must be secure & can be automated to ensure compliance with retention period requirements.

If a third-party data processor is responsible for handling personal data collected by JOE & THE JUICE, it is essential that the third-party data processor has established policies & procedures in place for the secure disposal of data. This must be ensured by each department when reviewing the provider's Data Processing Agreement, which must be signed prior to engaging with the third-party provider.

7 Policy Violations

Any violations of this policy will be taken seriously and may result in disciplinary actions. Failure to comply with retention policies & procedures may constitute a breach of relevant privacy laws & has the potential to result in financial penalties for the business.