JAMES AND JAMES
eCOMMERCE FULFILMENT

Data Protection Policy

Summary

This policy defines rules, procedures, and measures to collect, use, and store personal data within GDPR and control and prevent unauthorised access to personal data.

This policy is intended:

- To ensure the security integrity and availability of all the company and customer data
- To establish the company baseline data security stance and classification schema
- That it should enable the firm to meet its own requirements for the management of personal information
- That it should support organisational objectives and obligations
- That it should impose controls in line with the firm's acceptable level of risk

- That it should ensure that the firm meets applicable statutory regulatory contractual and/or professional duties
- That it should protect the interests of individuals and other key stakeholders

and embodies the principles of:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage Limitation
- Integrity and confidentiality

Breach of the policy

A breach of this policy could have severe consequences to James and James Fulfilment, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse of data resulting in a breach of any part of this policy will result in disciplinary action at the discretion of the Senior Management of James and James Fulfilment.

Severe, deliberate or repeated breaches of the policy by any employee may be considered grounds for instant dismissal, or in the case of a James and James Fulfilment vendor, supplier or third party processor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Scope of the Policy

This policy applies to all data processed by James and James Fulfilment, and covers all employees and users of the data.

This document forms part of our conditions of employment for employees , contractual agreements for vendors, suppliers and third party processors.

Processing environment

This policy applies to:

Systems– an assembly of computer hardware and application software configured for the purpose of processing, handling, storing, transmitting and receiving data which is used in a production or support environment.

Applications – programs designed by (and for) system users and customers, supporting specific business-oriented processes or functions.

Networks – devices that are used to transport information between systems.

Data Protection Responsibilities

The Technology Team are responsible for:

- Defining the security requirements controls and mechanism for the Platform ("ControlPort")
- Defining the methods and guidelines used to identify and classify all data assets
- Defining the procedures for identifying data owners for all data assets
- Defining the labeling requirements for data assets
- Defining procedures for data usage processing transmission storage and disposal
- Facilitating the evaluation of new regulatory requirements and best practices

In addition, other departments within James and James Fulfilment also have various responsibilities for ensuring compliance with this policy, such as:

- Individual departments must ensure that their staff comply with this policy.
- Ensure that adequate logs and audit trails are kept of all data access.
- The Senior Management Team is responsible for communicating business requirements and issues for business processes and the data those include to ensure their correct data classification.
- The Senior Management Team is responsible for regularly evaluating the data classification schema for consistent application and use.

Data Classification

The Senior Management Team is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage.

All data found in the processing environment must fall into one of the following categories:

- Confidential - only Senior Management Team and specific, defined and required persons have access
- Restricted - designated employees have access
- Internal - all employees have default access
- Public information - everyone has access

To ensure the security and integrity of all data, the default classification for all data not classified by its owner must be Restricted.

Data Ownership

In order to classify data, it is necessary that an owner be identified for all data assets. The custodian of data is responsible for classifying their data. The Senior Management Team is responsible for delegating the development, implementation, maintenance and procedures for identifying all data assets and associated owners.

Third Party Processors

Where James and James Fulfilment pass data to third parties for order fulfilment and address verification purposes, we validate said parties operate in accordance with our own Data Protection Policy and accord our agreement with theirs, including, but not limited to:

Metapack	https://www.metapack.com/en_gb/legal/data-processing-agreement/
DHL	https://www.dhl.com/content/dam/downloads/g0/legal/summary_dpdhl_privacypolicy.pdf
DeutschePost	https://www.dhl.com/content/dam/downloads/g0/legal/summary_dpdhl_privacypolicy.pdf
Intersoft	https://intersoft.co.uk/privacy-policy-cookie-notice-intersoft/
SmartyStreets	https://www.smartystreets.com/legal/privacy-policy
EasyPost	https://www.easypost.com/privacy
Norsk	https://norsk.global/wp-content/uploads/2020/11/Norsk-Data-Protection-Policy-01-Ocober-2020.pdf

Data Usage

All users that access James and James Fulfilment or customer data for use must do so only in conformance to this policy. Only uniquely identified, authenticated and authorized users must access and use data.

Data should be used only for the stated purpose of its collection or generation. Any purpose outside the defined scope will be considered “misuse of data”.

Each user must ensure that James and James Fulfilment data under their control is properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilised to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Storage

Data will only be stored for the time period necessary to fulfil its purpose, or to meet legal requirements. Data stored must be secured with encryption. Role Based Access Control (RBAC) mechanisms must be used to ensure only authorised users can access data to which they have been granted explicit access rights.

Data Transmission

Data transmitted must be secured with encryption. Specific cryptographic mechanisms are noted in the Information Security Policy. No data can be distributed in any media from a secured area without proper approvals.

Data Disposal

The Senior Management Team develops and implements procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques. Data should be disposed of in a secure manner so that it is completely destroyed and no information can be obtained from the waste.

Policy Review

It is the responsibility of the Senior Management Team to facilitate the review of this policy on a regular basis. This policy will be reviewed Annually. Last updated: 2021-04-06