# JOE & THE JUICE

# GDPR HANDBOOK FOR EMPLOYEES

**Title:** GDPR Handbook for Employees
**Effective Date:** October 2025
**Review Date:** October 2026
**Process Owner:** Compliance
**Approved by:** Head of Global Risk, Compliance & Safety

# About this document

## Document history

| Date | Version | Release Notes | Author |
|---|---|---|---|
| **September 2023** | 1.0. | | |
| **June 2024** | 1.1 | | |
| **7 October 2025** | 2.0 | | • Bree Bakaric |

## Contributors

| Name | Role |
|---|---|
| • **Bree Bakaric** | • Senior Data Privacy & Compliance Associate |

## Reviewers

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

# TABLE OF CONTENTS

# INTRODUCTION

JOE & THE JUICE is subject to data protection obligations originating from EU regulation such as the General Data Protection Regulation (“GDPR”), UK GDPR, Californian regulations such as the California Privacy Rights Act (“CRPA”) and California Consumer Privacy Act (“CCPA) & various other requirements under national laws.

JOE & THE JUICE must ensure compliance with those requirements in order to protect the personal data we process. Privacy compliance is a keystone in gaining & maintaining the trust of our customers, suppliers, & employees & thus, ensuring JOE & THE JUICE’s business in the future.

In order to ensure compliance with applicable data protection legislation, JOE & THE JUICE has adopted this handbook for the processing of personal data within JOE & THE JUICE.

Employees must comply with this handbook when processing personal data within JOE & THE JUICE. This GDPR handbook has been designed to provide you with the necessary knowledge regarding fundamental data protection rules.

If you have any questions regarding the content of this policy, please contact the privacy team at privacy@joejuice.com.

# 1 WHAT IS PERSONAL DATA?

Personal data is all information which can be attributed to a specific individual (the "data subject"). Personal data covers a broad range of information & can be classified as either general information or sensitive personal data. **Some** examples of personal data are:

| **General Personal Data** | **Sensitive Personal Data** |
|---|---|
| Identification information – name, phone number, address, date of birth, email address | Health information |
| Work, education & employment conditions – education, salary, job title, tax information, sick leave etc. | Racial or ethnic origin |
| Banking details including bank accounts & credit card details | Genetic & biometric data |
| Gender | Political, religious or philosophical beliefs |
| IP address | Sexual orientation or relations |
| Marital status, dependents, emergency contact details | Trade union membership |
| | Videos & Photographs – including CCTV |
| | Confidential information – such as national identification numbers |
| | Criminal offences/records |
| | Geolocation |

Although information regarding companies/businesses is not technically personal data, information relating to your contacts within third party vendors/contractors is classified as personal data.

JOE & THE JUICE collects & processes personal data for a variety of legitimate business purposes, including but not limited to:

- Recruitment
- Managing all aspects of employment
- Establishment & management of customer & supplier relationships
- Performance of contracts
- Execution of orders
- Customer service
- Communication & Marketing

**KEY TAKEAWAY: Personal data is any data that could be used to identify an individual.**

# 2 WHAT IS DATA PROCESSING?

Data processing includes any form of handling personal data from the time the data is collected until it is deleted. **Some** examples of data processing include:

- Collecting
- Recording
- Organising
- Structuring
- Sharing
- Disclosing
- Storing
- Hosting
- Cleaning
- Altering
- Using
- Restricting
- Combining
- Archiving
- Making available
- Deleting

**Some** examples of daily activities which include data processing are:

- Sending an email or chat message to a colleague or supplier
- Creating records (documents/spreadsheets) of third-party contacts
- Sending marketing material to customers
- Use of CCTV in stores & offices
- Conducting customer surveys
- Processing employee salaries

**KEY TAKEAWAY: Data processing is essentially any activity that involves you handling data of any kind.**

# 3 LEGAL BASIS FOR PROCESSING DATA

All processing of personal data requires a legal basis to ensure the processing is authorised and lawful. The main legal bases for processing personal data within JOE & THE JUICE are as follows:

1) The performance of a contract
2) Legal obligation
3) Consent from the data subject
4) Legitimate business interest

It is essential that the processing of personal data is based on the right legal basis to ensure it is lawful. It is also necessary that the data subject is provided with sufficient information about the data processing that we intend to do.

The legal bases for processing personal data depends on whether the data is classified as general or sensitive.

1) *Performance of a Contract*

   JOE & THE JUICE is entitled to collect & process non-sensitive personal data which is necessary for the performance of a contract, including orders, supplier contracts & employment agreements.

2) *Legal Obligation*

   JOE & THE JUICE must comply with various legal obligations & requirements under various national laws. Such legal requirements will then form the legal basis for JOE & THE JUICE to collect, register &/or make available certain types of personal data concerning employees, customers, etc. as part of compliance with requirements e.g. tax reporting.

   It is important to note whether the legislation allowing or requiring JOE & THE JUICE to process certain personal data set out requirements in relation to storage, disclosure, & deletion of the personal data

3) *Consent*

   Consent may not be used as an alternative to other legal bases if the data subject does not have an actual opportunity to withdraw their consent. If you are processing

personal data based on the data subject's consent, you must be able to demonstrate that the data subject has consented to such processing. The consent must be:

- **Voluntary**: the data subject must not feel pressured to provide consent)
- **Specific & unambiguous**: the data subject must be aware of the scope of their consent.
- **Informed**: the data subject must be provided with information regarding the type of personal data processed, the purpose of processing, any transfers of their personal data etc.

In order to process sensitive personal data, the data subject's consent must be **explicit.** This means that the data subject must by a statement or clear positive action (such as opting in or clicking consent) signify that they agree to the processing.

Data subjects are entitled to withdraw their consent at any time, upon which we must stop processing their data, unless we are obliged/entitled to do so on another legal basis.

4) *Legitimate Business Interest*

The processing of personal data may also be based on JOE & THE JUICE's legitimate business interest, which requires a "balance of interest" test.

This means that we are allowed to process non-sensitive personal data if the processing is necessary for the purposes of our legitimate business interests & those interests are not overridden by the interests of the data subject.

In order to process this data, the data subject must be provided details of our legitimate business interest prior to processing their personal data. The 'legitimate business interest test' can be broken down as follows:

(a) **Purpose test:** is there a legitimate interest behind the processing?

(b) **Necessity test:** is the processing necessary for that purpose?

(c) **Balancing test:** is the legitimate interest overridden by the individual's interests, rights or freedoms?

If you are in doubt of the legal basis for a specific processing activity, please contact the privacy team at privacy@joejuice.com.

**KEY TAKEAWAY: When you process personal data, you must first identify at least 1 of 4 legal bases for doing so.**

# 4 DATA PRIVACY PRINCIPLES

There are 7 main principles, as follows, which govern the processing of personal data & must be followed in respect of all processing activities:

1) Lawfulness, fairness & transparency
2) Purpose limitations
3) Data minimisation
4) Accuracy
5) Storage limitation
6) Integrity & confidentiality
7) Accountability

These 7 principles must guide all processing activities of personal data by JOE & THE JUICE employees.

| **Principle** | **Guide** |
|---|---|
| LAWFULNESS, FAIRNESS & TRANSPARENCY | All personal data must be processed lawfully, fairly & in a transparent manner. |
| PURPOSE LIMITATION | All personal data must be collected for specified, explicit & legitimate purposes & not processed in a manner that is incompatible with those purposes. |
| DATA MINIMISATION | Personal data must be adequate, relevant & limited to what is necessary in order to fulfil the purpose for which it is processed (this requires ensuring that the data collected is both *necessary/relevant* & *proportional* to the purpose for which it is collected). |
| ACCURACY | Personal data must be accurate & kept up to date. Every reasonable step must be taken to ensure that personal data is accurate & where inaccurate, rectified or where appropriate, deleted. |
| STORAGE LIMITATION | Personal data must not be kept for longer than is necessary for the purposes for which it was collected. When retention of |

| | |
|---|---|
| | personal data is no longer required to fulfil the purpose, it must be erased or made anonymous. |
| INTEGRITY & CONFIDENTIALITY | Personal data must be processed in a manner that protects the personal data against unauthorised or unlawful processing & against accidental loss, destruction or damage. This requires the implementation of technical or organisational security measures. |
| ACCOUNTABILITY | We must be able to demonstrate that we comply with data processing principles by documenting that all employees follow these rules & complete data privacy training. |

When JOE & THE JUICE determines the purpose & means of processing personal data, we are acting as the data controller, meaning we decide why the data is collected & how it is used. When we collect information directly from customers, third parties or employees, we are acting as the data controller & are legally responsible for ensuring data protection compliance.

**KEY TAKEAWAY: You must consider all 7 data privacy principles before you process any personal data.**

# 5 RECORDS OF PROCESSING ACTIVITIES

JOE & THE JUICE must maintain records of all data processing activities to ensure compliance with GDPR. These records must include the following information:

- The name & contact details of JOE & THE JUICE
- The purpose of the processing
- A description of the categories of data subjects & categories of personal data
- The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if relevant, the documentation of suitable safeguards
- The envisaged time limits for erasure of data
- A description of the technical & organisational security measures in place to protect the data

The JOE & THE JUICE Privacy team maintains our records of processing activities, which requires input from all business departments regarding their current & new processing activities.

**Identification of new processing activities**

Before any new activity involving the collection & processing of personal data is initiated, the risk of the processing activity must be assessed. In accordance with relevant legislation, JOE & THE JUICE has a risk-based approach to the processing of personal data. This means that the risk must be assessed in relation to the rights & freedoms of individuals.

JOE & THE JUICE must on an on-going basis assess the risk of processing personal data in order to identify cases where a certain type of processing imposes a high risk. Each risk assessment is specific, however, in general, any processing of sensitive personal data poses a higher risk to the data subject as the consequences of a breach of that data are greater.

Each department is, in cooperation with the Privacy team, responsible for documenting the processing of personal data according to this handbook, which requires each department to notify Compliance of any new data processing activities they wish to start.

For potentially higher risk data processing activities, a Data Protection Impact Assessment (DPIA) is required under GDPR. The purpose of a DPIA is to protect individuals' rights & freedoms with respect to their personal data & supports risk mitigation by identifying the ways

to reduce potential privacy risks before launching a new project. DPIAs are generally required in the following circumstances:

- When there is large-scale monitoring of people.
- Processing of sensitive personal data.
- Automated decision-making or profiling is involved.
- Surveillance of public areas or use of CCTV.

All new products, services, technical solutions, etc. must be developed so that they meet the principles of **data protection by design & data protection by default**.

Data protection by design means that when designing/configuring new products or services due consideration to data protection is taken.

Data protection by default requires implementation of relevant data minimisation techniques to ensure processing of personal data is limited to each specific purpose.

**KEY TAKEAWAY: When you wish to process personal data for a new purpose, please notify the Privacy team who will assist you in creating a record of this processing activity.**

# 6 USE OF DATA PROCESSORS

A data processor is an individual or organisation (e.g. – a software platform provider) that processes personal data on behalf of JOE & THE JUICE (as the data controller) in accordance with our instructions (see Appendix A for a comparison of Data Controllers v. Data Processors).

When JOE & THE JUICE outsources the processing of personal data to data processors, JOE & THE JUICE must ensure that the data processor as a minimum applies the same degree of data protection as we do. If this cannot be guaranteed, JOE & THE JUICE will choose another data processor.

For every data processor that you wish to engage with, JOE & THE JUICE must enter into a written Data Processing Agreement/Addendum (DPA) with the processor before making any personal data available to them. This ensures that the data processor is only processing the personal data in accordance with our instructions & mitigates certain privacy risks. Where possible, these DPAs must be signed by both a JOE & THE JUICE representative & the data processor.

Examples of data processors include the following:

- Technology & Cloud services: Amazon Web Services, Microsoft 365, Dropbox
- Email & Marketing services: Mailchimp, Sendgrid, Braze
- HR & Payroll services: ADP
- Customer Support tools: Zendesk
- Analytics & Ad platforms: Google Analytics, Facebook business tools
- E-commerce & Payment Processing tools: Stripe, Shopify, Tap

Before engaging with a new data processor, you must contact the Privacy team who will assess the risks associated with this data processor & the processing activity you wish to engage in.

**KEY TAKEAWAY: When you wish to engage with a new data processor, please notify the Privacy team who will assist you in assessing the associated privacy risks.**

# 7 COLLECTION & USE OF PERSONAL DATA

You can only collect personal data when there is a defined purpose for the collection of the data & its intended use. The purpose for collection of one's personal data must be specific enough to understand why we require the data.

When determining whether we can collect personal data, it must always be assessed as to whether the specific data is relevant & necessary for the intended purpose. This means that we cannot simply collect personal data from customers, employees or third parties for the sake of having that data, but rather, we must need that data in order to satisfy a purpose or perform a specific task.

As noted above, before collecting personal data, we must also ensure that there is a legal basis for processing the data.

When we collect personal data, the data subjects must be informed prior as to how we intended to use & process their data. We are then only allowed to use that personal data for the intended purpose we specified, which means you cannot use the data for another purpose.

**KEY TAKEAWAY: Before you process personal data, you must have a defined purpose for doing so and ensure that the data you are collected is necessary in proportion to your purpose.**

# 8 SHARING & DISCLOSURE OF PERSONAL DATA

Sharing & disclosing personal data is considered as a separate function to collecting & using personal data. This means that before sharing personal data with another party, you must ensure that it falls within the purposes for which the data was collected & that there is a legal basis for the sharing/disclosure.

The processing of personal data within JOE & THE JUICE is subject to confidentiality & personal data is only disclosed to recipients who act as individual data controllers if the disclosure serves a legitimate business purpose.

Before disclosing personal data to others, first consider whether the recipient is another JOE & THE JUICE employee. Other employees of JOE & THE JUICE are allowed to receive personal data if it is shared for a work-related purpose.

You cannot share/disclose personal data with a third-party data processor without having informed the data subject of this, unless a specific exception applies (i.e. – specific legislation requires you to disclose this information to the authorities). If you receive a request from authorities to share personal data we have collected at JOE & THE JUICE, please contact the Privacy team prior to doing so.

**KEY TAKEAWAY: If a third party requests that you share personal data with them, you must first contact the Privacy team.**

# 9 STORAGE, RETENTION & DELETION OF PERSONAL DATA

## Storage

It is important that storage of personal data is done in a secure manner to prevent it from being lost, misused or accessed by unauthorised third parties. As a general rule, your email cannot be used as your main filing tool for personal data. If an email you receive/send contains confidential or sensitive personal data, the email must be deleted or, if required, saved in the relevant IT system & then deleted from your email. If there is no suitable IT system to save personal data, it should be stored in a subfolder in the email system.

Storage of documents containing personal data on personal drives & Dropbox must be limited to what is strictly necessary. If a system exists for handling or storing these types of documents, it is essential that only those who have a work-related need to access the documents can do so. These documents must be stored in a structured form so that you can easily identify the documents.

It is our policy that confidential & sensitive personal data may not be stored in physical form, such as on external or transportable drives (USBs, hard drives etc.) or in physical documents. If non-sensitive personal data must be stored in physical form, it must be limited to what is strictly necessary & you must ensure that these physical forms/drives are stored securely & only accessible by those who need access. These types of hard-copy items (such as folders, physical notes etc.) must be stored in locked cabinets, drawers or similar facilities & must not be accessible by other employees.

## Retention and Deletion

As a general rule, JOE & THE JUICE may only keep personal data for as long as is necessary to fulfil the purpose for which it was collected or when it is no longer required to store the personal data in accordance with applicable legislative requirements (e.g. – in relation to tax or employment law).

If personal data is found to be inaccurate or unnecessary for the purpose, you must delete or amend the personal data as soon as possible.

Each department must determine retention periods for the personal data they collect & store with respect to the purpose for which they use the data. These retention periods must be strictly adhered to. Please refer to JOE & THE JUICE's Data Retention Policy here.

**KEY TAKEAWAY: You must store all personal data in a secure manner and ensure that it is deleted in accordance with our Data Retention Policy.**

# 10 SECURITY MEASURES

It is essential that together with IT, each department at JOE & THE JUICE implements safeguards & security measures to maintain the security & integrity of the personal data they collect & use. Security measures may include technical measures, which are technology-based protections or organisational measures, which include policy, procedures & people-focused controls.

Examples of technical measures include encryption, pseudonymisation & anonymisation, individual passwords, access logs, session timeout & auto-logout, firewalls, access controls (such as multi-factor authentication), regular back-ups.

If it is possible to anonymise or aggregate the personal data to an extent where it is no longer possible for anyone to identify the persons behind the data, then the data is no longer considered to be personal data. However, pseudonymised data is still considered personal data.

Examples of organisational measures include data protection policies, employee training, data minimisation & retention policies, incident response plans & regular audits & reviews of personal data collected.

Each department should utilise both technical & organisational measures to ensure the security of the personal data they collect, store, use & disclose.

**KEY TAKEAWAY: You must utilise security measures to ensure that any personal data you process is only accessible by those who need access for the defined purpose.**

# 11 TRANSER OF DATA TO A THIRD COUNTRY

There are specific rules that apply under law to the transfer of personal data between countries outside of the European Union (EU) / European Economic Area (EEA).

Transfers of personal data to a country outside of the EU/EEA includes both situations where the data is physically transferred, situations where it is simply accessed from a location outside of the EU/EEA (remote access) or where data processors outside of the EU/EEA are utilised for data processing/storage.

If the recipient of personal data is located outside the EU/EEA, in a country which is not approved by the EU Commission as a secure third country,[1] or the processing of personal data is carried out outside the EU/EEA, or personal data may be accessed outside the EU/EEA, the personal data may only be transferred if a proper transfer tool exists.

The transfer tool may take the form of a transfer agreement based on the EU Commission's Standard Contractual Clauses, an adequacy decision or binding corporate rule. Please contact the Privacy team if this is required.

Under GDPR, an EU-US Data Privacy Framework also exists which allows the transfer of personal data from the EU to US companies & organisations if they have signed up to the Data Privacy Framework by means of certification.[2]

If no adequacy decision exists for a country, JOE & THE JUICE must ensure that the personal data will be sufficiently protected by the recipient via the use of standard contractual clauses. Between JOE & THE JUICE entities, this can be ensured via binding corporate rules. This can also be ensured through the commitment to comply with codes of conduct & the use of a Data Processing Agreement/Addendum.

**KEY TAKEAWAY: You must not transfer personal data to a third party located outside of the EU without having an appropriate transfer mechanism in place. Please contact the Privacy team for assistance if you wish to transfer personal data to a third party located outside of the EU.**

[1] Secure third countries which ensure an adequate level of protection are Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom & South Korea. Data transfer to these countries is expressly permitted.

[2] Data Privacy Framework

# 12 RIGHTS OF DATA SUBJECTS

Under GDPR, data subjects are given a number of rights in respect of their personal data. When we collect personal data, we are required to inform data subjects about the following:

- The name & the contact details of JOE & THE JUICE
- The purposes of the processing for which the personal data is collected
- The legal basis for the processing
- The categories of personal data collected
- The legitimate interests pursued by JOE & THE JUICE, if the processing is based on a balancing of interests
- The recipients or categories of recipients of the personal data, if any
- Whether JOE & THE JUICE intends to transfer personal data to a third country & the legal basis for such transfer
- The period for which the personal data will be stored
- The existence of their rights under GDPR – to access, to rectification/erasure of personal data, to restriction of processing, to object to processing (set out below)
- Whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract as well as whether the data subject is obliged to provide the personal data & of the possible consequences of failure to provide such data
- Whether automated decision-making, including profiling, is taking place
- The right to lodge a complaint with a supervisory authority
- The right to withdraw consent to processing

Under EU and UK GDPR, data subjects can exercise the following rights in relation to their personal data:

1. Right to be Informed (Articles 13 & 14).
2. Right of Access (Article 15).
3. Right to Rectification (Article 16).
4. Right to Erasure (Article 17).
5. Right to Restriction of Processing (Article 18).
6. Right to Data Portability (Article 20).

7. Right to Object (Article 21).
8. Rights regarding Automated Individual Decision-making, including profiling (Article 22).

Under the CCPA/CPRA, data subjects hold the following rights in relation to their personal data:

1. Right to Know
2. Right of Access
3. Right to Erasure/Deletion
4. Right to Object
5. Right to Data Portability
6. Right to Opt-Out
7. Right to Rectification
8. Right to Non-Discrimination

If you receive a request from a data subject to exercise one of the rights above, please follow our JOE & THE JUICE Data Subject Requests Process (found here) & notify the Privacy team (privacy@joejuice.com).

Under GDPR, any request received from a data subject must be answered as soon as reasonably possible & no later than 1 month from receipt. Requests must be handled in accordance with JOE & THE JUICE's privacy policies & our Data Subject Requests Process.

Privacy Policies

JOE & THE JUICE has an internal employee privacy policy which provides employees with information about how their personal data is processed (available on e-Campus). We also have an external privacy policy describing how JOE & THE JUICE processes personal data concerning visitors to websites, business partners, customers, subscribers to newsletters etc. (available on the company website).

**KEY TAKEAWAY: If you receive a request from an ex-employee, customer or other third party for access to the personal data we hold about them, please contact the Privacy team for assistance in providing a response.**

# 13 PERSONAL DATA BREACHES & INCIDENT RESPONSE

A personal data breach occurs when a security breach causes the accidental or unlawful loss, alteration, deletion, unauthorised disclosure of/access to, personal data.

Examples of data breaches include cyberattacks, stolen passwords, accidental sending of information to an incorrect recipient, malicious software downloaded.

If a data breach occurs, please follow the procedure set out in JOE & THE JUICE'S Data Breach Response Process, found here.

**KEY TAKEAWAY: If you identify a data breach has occurred, please notify the Privacy team immediately as there are strict timeframes that we must comply with when this occurs.**

# 14 INFRINGEMENT

All JOE & THE JUICE employees are obliged to comply with this GDPR Handbook, as amended from time to time. The high level of data protection within JOE & THE JUICE can only be ensured if all employees are conscious of their responsibility to comply with our data protection policies & guidelines.

Any breaches of the guidelines in this GDPR Handbook may result in formal warnings or other employment sanctions.

Please address any questions about the content of the GDPR Handbook to the Privacy team, who are always happy to guide you in respect of best practice (privacy@joejuice.com).

# APPENDIX A: COMPARISON OF DATA CONTROLLERS V DATA PROCESSORS

| Feature | Data Controller | Data Processor |
|---|---|---|
| **Role** | Determines the purposes & means of processing personal data (the 'how' & 'why') | Processors data on behalf of the controller |
| **Decision-making** | Decides & controls about what personal data is collected, why & how it is used | Must follow instructions of the controller, has no autonomy in decision-making regarding personal data use |
| **Responsibility** | Legally responsible for overall compliance with data privacy laws | Responsible for implementing appropriate technical & organisational measures |
| **Data Ownership** | Controls data use & management | Does not control data, merely handles it as instructed by data controller |
| **Contract Requirements** | Must ensure DPAs & contracts in place with data processors | Must operate under a contract that clearly sets out obligations & limitations |
| **Examples** | Joe & the Juice deciding what data to collect from customers for marketing purposes | A cloud storage provider that stores customer & employee data for Joe & the Juice<br><br>Examples include cloud hosting providers, payroll services & marketing agencies |
| **Liability under GDPR** | Fully liable for compliance, even for processor actions if not properly managed | Liable for its own non-compliance & any breach in respect of controller's instructions |