
# Employee Data Protection Policy

## Contents

## 1. Purpose, Scope and Users

This Policy regulates the management of Personal Data relating to the employees of KubeNet ("The Company"), and provides rules and procedures which apply to all departments and individuals within the Company, aimed at ensuring that employee Personal Data is processed and protected properly in all countries and regions.

This Policy applies to the Processing of employee Personal Data by any department or individual within the Company, in all countries and regions.
"Company" refers to Kubet and all wholly-owned subsidiaries directly or indirectly controlled by it; but excludes joint venture companies.

The users of this document are all employees of The Company.

## 2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Information Security Policy
- Employee Personal Data Protection Policy
- Data Retention Policy
- Data Protection Officer Job Description
- Guidelines for Data Inventory and Processing Activities
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Guidelines
- Cross Border Personal Data Transfer Procedure
- Breach Notification Procedure

## 3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

**Personal Data:** Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Sensitive Personal Data:** Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Data Controller**: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

**Processing**: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

## 4. General Principles for Processing Employee Personal Data

### 4.1 Lawfulness, Fairness and Transparency

Employee Personal Data must be processed lawfully, fairly, and in a transparent manner in relation to the employee.

### 4.2 Purpose Limitation

Employee Personal Data must be collected for specified, explicit, and legitimate purposes, and should not be further processed in a manner that is incompatible with those purposes.

### 4.3 Data Minimization

Employee Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

### 4.4 Accuracy

Employee Personal Data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that employee Personal Data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

### 4.5 Storage Period Limitation

Employee Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data are processed, according to the Data Retention Policy.

### 4.6 Integrity and confidentiality

Taking into account the state of technology and the available security measures, the cost of implementation, and the likelihood and severity of privacy risks, appropriate technical and organizational measures must be used to ensure appropriate security for Personal Data, including protection against accidental or unlawful destruction, loss, alteration, unauthorized access, or disclosure.

### 4.7 Accountability

The Company, as Data Controller for employee Personal Data, shall be responsible for and be able to demonstrate compliance with the principles outlined above.

## 5. Legitimate Purposes for Processing Employee Personal Data

Company departments or individuals may process employee Personal Data for legitimate purposes which include but not limited to:

**Human resources management.** This purpose includes human resource management activities carried out during recruitment or the performance of an employment contract, such as interviews, on boarding, termination of employment, attendance, performance management, compensation and benefits, training, employee services, health and occupational safety, and other activities for the purpose of human resource management or protecting the vital interests of employee.

**Other business operations.** This purpose includes business activities such as managing travel and expenses, managing company assets, providing IT services, information security, conducting internal audits and investigations, fulfilling the obligations of business contracts, legal or business consulting, and preparing for legal litigation, etc.

**Compliance with the law.** The Processing of employee Personal Data in order to comply with a legal obligations, for example: the disclosure of employee Personal Data to a tax authority in order to comply with applicable tax laws.

## 6. Requirements for the Processing of Employee Personal Data

Any Processing of employee Personal Data by Company departments and individuals must be for a legitimate purpose, and must comply with the following requirements:

### 6.1 Notification to Employees

For the purpose of transparency of employee Personal Data Processing, when a Company department or individual collects the Personal Data of an employee, the employee should be notified of the types of data being collected, the purpose and types of Processing, the employee's rights, and the security measures taken to protect the Personal Data. Notification may take the form of the publication or updating of statements on the protection of employee Personal Data, for example: the insertion of terms on employee Personal Data protection in employment contracts by the Employee Relationship Department/HR.

### 6.2 Employee Choice and Consent

In principle, the Company may Process employee Personal Data for a legitimate purpose as an employer and generally it may do so without obtaining the consent of the employee, to improve the efficiency of internal operation.

Human resource management activities such as interviews, on boarding, termination of employment, attendance, compensation and benefits, employee services, health and occupational safety may involve the Processing of Sensitive Personal Data. If country specific laws or regulations govern these issues (for example, obtaining the consent of the employee), the Company shall take these laws or regulations into account.

### 6.3 Collection

Company departments and individuals must collect employee Personal Data for legitimate purposes, and must comply with the principle of Data Minimization. If the Personal Data of a job candidate or employee is collected from a third party (e.g. recruitment or background check agencies), the Company must make best efforts to ensure that the third party obtained the Personal Data by legitimate means.

No Company department or individual may collect Personal Data of job candidates or employee in a way which is inconsistent with the law or business ethics.

### 6.4 Use, Retention, and Disposal

Company departments and individuals must use, retain, and dispose of employee Personal Data in a manner which is consistent with the notification to the employee. It must also ensure its accuracy, integrity, and relevance. They must take appropriate security measures to protect the employee Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized access, or disclosure according to Information security policy and other documents that describe data security.

Company departments and individuals must not unlawfully destroy or alter employee Personal Data. They must not access, sell, or provide employee Personal Data to any third party unlawfully or without authorization.

In the course of business operations, the Data Protection Officer will decide whether the employee Personal Data will be Processed in the following ways to minimize data protection risk: employee Personal Data may be anonymized for the purpose of irreversible de-identification; or data may be aggregated into statistical or survey results.

### 6.5 Disclosure to Third Parties

When Company departments and individuals need to disclose employee Personal Data to a supplier, business partner, or other third party, they should seek to ensure that the supplier, business partner or other third party will provide security measures to safeguard employee Personal Data that are appropriate to the risks associated. They should also require the third party to provide the same level of data protection as the Company by contract or other arrangement.

Besides, when Company departments and individuals disclose employee Personal Data in response to a request from a law enforcement agency or judicial authority, they should first inform the Company Direction which is authorized to make a coordinated effort to handle the request.

### 6.6 Employee Access

Company departments must provide reasonable means for employees to access Personal Data held about them and allow employees to update, correct, erase, or transmit their Personal Data if appropriate or required by law. When responding to an employee request for access, Company departments may not provide any Personal Data until they have verified identity of the employee.

The Company needs to make sure that they know the identity of the person making the request before they can send the personal data to the individual.

## 7. Responsibilities

The Company Directors is responsible for the management of employee Personal Data protection.

## 8. Response in the Event of Non-compliance

Any person who has knowledge of a data breach involving employee Personal Data should report it to the relevant persons within the Company. When is necessary to report the data breach outside the Company, please follow the Data Breach Response and Notification Procedure.

However, if required by the local law of the country where the data breach occurred, the person designated in the Data Breach Procedure must report the incident to the regulator and/or stakeholders within the reporting period specified by law.

## 9. Accountability

Any individual who breaches this Policy may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

## 10. Exceptions and Variations

Company departments and individuals should also refer to this Policy when Processing the Personal Data of other personnel. "Other personnel" includes:
(1) individuals seeking employment at Company;
(2) individuals who have previously been employed by Company;
(3) other non-employee of Company who work at Company facilities (such as employee of cooperating partners, consultants, interns)

## 11. Owner and Contacts

The Company Director is the owner of this Policy, and must interpret and manage it.

## 12. Managing records kept on the basis of this document

| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
|---|---|---|---|---|
| Employee Records | Secure File Server | Julie Inglis, Director | Only the authorized persons are allowed to access these contracts. | 3 years after termination of contract |