

# Employee Privacy Statement

*Updated on 11 March 2020*

## 1 Controller

Eezy Henkilöstöpalvelut Oy (hereinafter referred to as "EEZY")  
Business ID: 2632054-7  
Satakunnankatu 24 A, 33210 Tampere, Finland  
Tel.: +358 3 31229200

## 2 Contact details of the person responsible for data protection

Attorney Otto Michelsen  
c/o Eezy Kevytyrittäjät Osk  
Telephone: 09 4242 1559  
E-mail: [tietosuoja@vmp.fi](mailto:tietosuoja@vmp.fi)

## 3 Privacy statement description

This privacy statement in accordance with Articles 13 and 14 of the General Data Protection Regulation (679/2016/EU) and the Finnish Data Protection Act (1050/2018) describes how the controller processes the personal data of employees in an employment relationship with the controller.

## 4 Personal data to be processed

The following personal data categories are collected and processed of the data subjects:

- Data subjects' identification and contact details, such as the name, identification number, address, telephone number, citizenship, gender, bank contact details, contact details of a close relative for emergencies and other necessary data for identifying the data subject (for instance, copy of an identification)
- Data related to the data subject's employment relationship, such as
  - job application and other data related to the application process (education and degree information, work and professional experience, qualifications and information from suitability assessments, among other things)
  - employment contracts and other possible agreements and undertakings related to the employment relationship
  - data about the content of the work tasks, such as job title
  - data regarding development in work tasks (for instance, data about further training)
  - data about work performance (for instance, qualifications and language skills)
  - data related to compensation paid based on the employment relationships (for instance, salary, employee benefits or other rewards and data related to them, taxation information and data about employer payments, travel invoices and kilometre allowances)
  - data about employer liabilities related to the employment relationship (for instance, data about the data subject's insurances)
  - data about occupational health care services, such as data about the employees' health if the data has been collected from the employee or

elsewhere with their written consent, and the processing of the data is necessary for clarifying salaries from a period of sick leave or other comparable benefits related to health, or to clarify if there is a justified reason for an absence from work, or if the employee specifically wants their work ability to be investigated based on data about their health

- data about unions, such as union memberships if the data has been collected at the employee's consent and the processing of the data is required for making union membership fee payments, for instance
  - data related to working time monitoring and absences (for instance, data from an access control system, sick leaves, annual leaves and other leaves or agreed-upon absences)
  - data related to working equipment and tools (for instance, data related to computers and other mobile devices appointed for the use of the person and their use, person's e-mail addresses and telephone numbers as well as data related to access cards and keys)
  - data of the rights to use related to work tasks and their login credentials
  - data about ending the employment (such as an agreement to end the employment, reference, data about retiring)
- Change data of the data subject's above-mentioned individualised personal data categories.

## **5 Regular sources of personal data**

Employees' personal data is primarily collected and updated from the employees. Personal data is also collected from information systems used to fulfil the obligations of the employee's employment and employer, such as the data produced by HR software.

With the data subject's consent, the controller may also collect personal data from other places. No consent is required if the controller obtains personal credit information or criminal record information to investigate the reliability of the person. The controller notifies the person in advance about acquiring this kind of information for investigating the reliability of the person.

## **6 Purpose and legal basis for the processing of personal data**

The controller processes personal data to fulfil tasks and obligations related to the employee's employment, such as tracking working hours and absences, payroll administration, access management and measures related to starting, managing, developing and ending the employment. Personal data may also be processed to create statistics and plan the controller's operations. Personal data may be processed for the above-mentioned purposes in companies that belong in the same group of undertakings as the controller.

In addition, personal data is processed for realising the controller's customer communications. Customer communications may be targeted to the data subjects also using the electronic means of communication, such as e-mail newsletters. The personal data provided by the employee may also be used to provide different benefits for the employees related to different work tasks and working life in general using an electronic means of communication and for profiling the employee unless the employee has forbidden profiling. You have the right to change the settings for collecting your data in the eezy.fi online service.

The legal basis for the processing of personal data is the legitimate interest created based on the employment between the controller and the employee and legislation related to handling

the controller's employer obligations, such as legislation about taxation, enforcement and statistics. The legal basis for processing special personal data is the data subject's consent.

## **7 Disclosure and transfer of personal data**

Personal data stored in the register may be disclosed as allowed and obligated by the valid legislation or with the data subject's consent to the public authorities who have a legal right to receive data from the register, such as the Tax Administration or the Social Insurance Institution of Finland and other parties who are related to managing matters related to employment, such as pension and accident insurance companies, unions and parties providing occupational health care services.

With the data subject's consent, personal data necessary for the employment may be disclosed to such partners of the data controller who the employee does different assignments for on behalf of the controller.

When the data subject uses online services provided by the controller's or another company in the same group of undertakings that require creating a username (such as discussion forums), the username selected by the data subject will be shown in these online service. The data subject may also decide to use their own name as a username.

In addition, personal data may be disclosed to such partners of the data subject that process personal data on behalf of the controller and instructed by the data controller. In these cases, the data controller's partner does not have the right to process the personal data on behalf of itself.

In addition, personal data of job applicants may be conveyed to Eezy Henkilöstöpalvelut Oy companies for the purposes of promoting employment upon the consent of the applicant.

Primarily, data is not transferred to locations outside the member states of the European Union or the European Economic Area unless necessary for the technical implementation of the data processing or the purposes of the processing of personal data. In these cases, requirements of the data protection legislation will be complied with in the transfer of data.

## **8 Protection of personal data**

The controller implements the appropriate technical and administrative data privacy measures for the protection of personal data. Personal data is stored in both electronic databases and manually maintained materials. Electronically processed databases are protected using firewalls, passwords and other technical measures generally accepted in the field of data privacy. Manually maintained and processed materials are located on premises with no unauthorised access.

Personal data may only be access by the specifically defined and identified people whose work performance requires the processing of personal data stored in the register. These people may access the system using their personal login credentials to the controller's internal network. Each user has signed a special login credential and confidentiality agreement.

## **9 Retention period of personal data**

The employee's personal data is stored only for as long as is required for the implementation of the purposes specified in this privacy statement, and for a maximum period of ten years after employment has ended. The retention period of ten years is based on the periods for filing a suit applied at the time of employing, such as the obligation to provide a referral as specified in the Employment Contracts Act.

## **10 Rights of the employee**

As the data subject, the employee has the following rights guaranteed by the data protection legislation:

1. The employee has the right to ask the data controller for access to their personal data and the right to ask for the said data to be rectified. The request for rectifying personal data must be individualised so that the error in the personal data may be observed and rectified easily.
2. The employee has the right to request the erasure of personal data pursuant to and within the limits of the data protection legislation.
3. The employee has the right to request the restriction of processing of personal data and to object to the processing of personal data pursuant to and within the limits of the data protection legislation.
4. The employee has the right to data portability or the right to receive their personal data in a structured and generally used format and transfer them to another controller pursuant to and within the limits of the data protection legislation.
5. The employee has the right to file a complaint with the local data protection authority (in Finland, [the Data Protection Ombudsman](#)) or another data protection authority in the European Union or the European Economic Area if the employee sees that the statutory rights related to the processing of their personal data have been breached.

Exercising the rights in sections 1–3 hereinabove can be done for data related to the employee's application process and partially for the data related to working (for instance, payslips and electronically signed employment contracts) in the eezy.fi service using personal login credentials. You can view, edit, store and transfer your personal data when you are logged in the eezy.fi service. If the above-mentioned actions are not possible due to a technical or other reason, the request for rectifying personal data must be individualised so that the error in the personal data may be easily observed and rectified by EEZY.

The employee may address the requests of exercising their above-mentioned rights to the contact person in charge of data protection.

## **11 Changes to the privacy statement**

The controller continuously develops its business operations and, therefore, reserves the right to change this privacy statement by notifying about it in its services and on its website at <https://eezy.fi/tietosuoja/>. Changes may also be based on changes in the legislation. The controller recommends that the employees check the content of the privacy statement regularly and from time to time again.