



## PRIVACY STATEMENT FOR AGENCY AND SECONDED EMPLOYEES

Last updated: April 12<sup>th</sup>, 2019

*Your privacy is important to us and we work hard to protect your information. This privacy statement which is based on the General Data Protection Regulation (EU) 2016/679 describes what personal data is being processed by Enersense, how it is processed and for what purposes.*

### 1. Controller of Personal Data (depending on the employer of the employee)

#### **Enersense International Oyj**

Business ID: 0609766-7  
Konepajaranta 2  
28100 Pori, FINLAND

#### **Enersense Engineering Oy**

Business ID: 2490497-9  
Konepajaranta 2  
28100 Pori, FINLAND

#### **Enersense Henkilöstöpalvelut Oy**

Business ID: 0844818-4  
Konepajaranta 2  
28100 Pori, FINLAND

#### **Enersense Technologies Oy**

Business ID: 2429163-1  
Konepajaranta 2  
28100 Pori, FINLAND

#### **HSE Management Group Oy**

Business ID: 2948437-9  
Konepajaranta 2  
28100 Pori, FINLAND

### 2. Contact Information for the Register

In case you have any questions or concerns related to the processing of personal data or the exercise of your rights under the General Data Protection Regulation you may contact our Data Protection Officer at: [dpo@enersense.com](mailto:dpo@enersense.com).

### 3. Name of the Register

External employee register ("**Register**"). The Register contains personal data of Enersense International Oyj and its group companies' ("**Controller**") agency and seconded employees ("**Data Subject**"), who are leased or sent to work for client companies.

### 4. The nature, purposes and the legal basis for the processing

The processing of personal data is necessary for fulfilling the rights and responsibilities in the employment relationship between the employee and the Controller. Procedures and

responsibilities related to these rights include e.g. work time monitoring, payment of salaries as well as proceedings related to the commencement and ending of employment.

For the above-mentioned purposes, the personal data may also be processed by the respective client companies for whom the employee works for and other companies belonging to the Enersense Group.

Based on data protection regulations, the Controller processes personal data on the following legal basis for processing:

Purpose of processing personal data	Legal basis for processing
<p>E.g. payment of salaries according to the employment agreement and disclosure of personal data to client companies of the Controller.</p>	<p><b>Employment agreement</b></p> <p>The processing of the personal data is based on the preparation and performance of the employment agreement between the employee and the Controller.</p>
<p>The Controller may process the personal data insofar as the personal data is being processed after the expiry of the employment relationship and the lawfulness of the processing is not based on the preparation and performance of the employment agreement or the fulfillment of the employer's statutory obligations. In this case, the legitimate interests are founded on the project-related nature of the employment relationships and the provision of employment after the expiry of the employment relationship.</p> <p>The transfer and disclosure of Personal Data to the Controller's affiliates is also based on the Controller's legitimate interest.</p> <p>Direct marketing is likewise based on the Controller's legitimate interest.</p>	<p><b>Legitimate interest</b></p> <p>Legitimate interest of the Controller exists in situations such as where the employee is in the service of the Controller. The Controller shall make sure that the processing of personal data is proportionate to the interests of the data subject and corresponds with his or her expectations.</p> <p>The data subject has the right to object the processing of personal data according to the requirements of the EU Data Protection Regulation, insofar as the processing is based on the legitimate interest of the Controller.</p> <p>The Controller has also conducted the balancing test as defined by the Data Protection Authority to ensure that the data subject's interests are taken into account.</p>
<p>E.g. the employer's obligation to notify the employee's salary information to the tax authority or the employer's right to respond to legal claims.</p>	<p><b>Legal obligation</b></p> <p>Personal data may be processed to fulfill the employer's requirements and obligations stated in laws, regulations or</p>

	decisions from authorities and supervisors.
The handling of special categories of personal data may be based the consent of the data subject.	<b>Consent</b> Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, which gives the Controller the legal basis to process personal data.
The transfer of personal data to countries of employment outside the EU/EEA may be performed on this legal basis.	<b>Conclusion or performance of a contract</b> The processing is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Controller and another natural or legal person.

## 5. Categories of Personal Data contained in the Register

The following categories of personal data concerning the data subject may be processed in the Register:

- Basic Details:
  - **Personal details** (first name and surname, social security number, date of birth, nationality, gender, copy of passport/ driving license, photograph of the employee)
  - **Contact details** (postal address, phone number, email address)
  - **Contact details of next of kin for emergencies** (name, relationship to the employee and phone number)
- Employment related details:
  - Employment agreement and other written commitments of the employee
  - Personal data related to:
    - **the substance of the employment relationship** (e.g. job title, length of employment and workplace)
    - **qualification, competence and special skills** (e.g. work permit, existence of driving license, criminal records, certificates and spoken languages)

- **work performance** (e.g. written warnings, memoranda of development discussions)
- **payments made under the employment relationship** (i.e. bank account number, salary details, daily allowances, bonuses, taxation information)
- **fringe benefits** (e.g. company apartment, company car and car fuel details)
- **information specifically on the leasing relationship or the secondment** (e.g. client company details, work code provided by the client and project length)
- **the employer's statutory obligations** (e.g. insurance information)
- **occupational health care** (e.g. information related to the employee's health)
- **monitoring of work time and absences from work** (e.g. daily working hours, sick leave periods, holiday periods and other absences from work)
- **work tools** (e.g. information related to computers and mobile devices given to the employee's possession, business phone number, business email address and information related to access cards)
- **access rights** (e.g. usernames and passwords, IP address information)
- **the ending of employment** (e.g. letter of notice, work certificate, information on retirement)

## 6. Storage of Personal Data

Personal data is stored as long as it is required for the purposes of processing determined in Section 4, as long as statutory obligations require storage of personal data, or until the data subject submits a deletion request concerning his or her personal data. However, personal data shall not be stored longer than **ten (10)** years from the expiry of the employment relationship, with the following exceptions:

- payroll and bookkeeping data for **ten (10) years** from the end of the accounting period in question as specified in the Accounting Act and other applicable legislation

## 7. Sources of Personal Data

Personal data is primarily collected from the employee. Personal data may also be collected from other sources upon the employee's consent. In case the Controller seeks to obtain credit details or criminal record details to ascertain the trustworthiness of the employee, the employee's consent is not needed. The Controller shall inform the employee before obtaining such information.

## 8. Transfer of Personal Data and the Categories of Recipients of Personal Data

Personal data shall not be transferred to third parties without the consent of the data subject. Notwithstanding the above, personal data may be transferred within the limits of

the purposes of processing determined above in the following circumstances:

**Within the Enersense Group:** Personal data may be transferred to affiliates of the Controller within the limits of the purposes of processing determined above.

**Client Companies:** Personal data may be transferred to those client companies of the Controller or its affiliates in whose assignments the data subject is or could be employed.

**Authorities:** In addition, personal data may be transferred based on applicable legislation or upon the consent of the data subject to authorities, who have a statutory right to receive personal data from the Register, e.g. tax authorities and KELA, and other entities connected to the management of employment related rights and responsibilities, e.g. accident and pension insurance companies and occupational health care providers.

**Transfers outside EU and EEA:** Personal data shall not be transferred outside the European Union ("EU") or the European Economic Area ("EEA") unless it is necessary in regards to the purposes of processing determined above. In case personal data is transferred outside the EU or the EEA, the Controller shall implement suitable safeguards in order to comply with the requirements of applicable data protection legislation. The Controller may for instance conclude an agreement with a Client operating outside the EU or the EEA in accordance with the standard data protection clauses adopted by the European Commission.

In the absence of an adequacy decision by the European Commission ensuring an adequate level of data protection in the receiving country, or appropriate safeguards, including binding corporate rules or agreements in accordance with standard data protection clauses, the Controller may transfer personal data outside EU and EEA, on the condition that the transfer is **occasional** and **necessary** for the conclusion or performance of a contract concluded in the interest of the data subject between the Controller and another natural or legal person. The aforementioned may be applied in cases in which the data subject is employed outside the EU/EEA, and the Controller has to transfer the necessary personal data to the client, local authorities or third-party service providers (e.g. apartment or car agencies) in order to comply with the employment agreement or agreement with the client company (user enterprise).

## 9. Security of Processing

The Controller has appropriate technical and organisational means of data security in order to safeguard data subjects' personal data from loss, misuse or other equivalent illegal access. Secure processing of personal data is ensured by providing instructions as well as implementing access management to provide access to designated employees of the Controller or its affiliates. Personal data is only processed by employees who have the right to do so within the framework of their work duties.

Data security is a central part of the core values of Enersense. Therefore, data security is evaluated and developed regularly.

## 10. Employee's rights as a data subject

The data subject can exercise their rights by contacting the data protection officer using the information in section 2. The data subject has the following rights as defined by the GDPR:

- The right to **obtain** confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data.
- The right to have incorrect or incomplete information **corrected or completed**.
- The right to request **erasure** of personal data concerning him or her.
- The right to **restrict** processing of personal data, when applicable according to the GDPR.
- The right to **receive** the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and the right to **transmit** those data to another controller.
- The right to **object** processing of personal data, **including direct marketing** according to the requirements of the GDPR.
- The right to lodge a **complaint** with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

## 11. Updates to this Privacy Statement

The Controller continuously develops its services, which is why the Controller reserves the right to change this Privacy Statement. Changes may also be based on amendments in legislation. The Controller recommends the data subject to review the content of the Privacy statement on a regular basis. The Controller may also, if necessary, notify the changes directly to data subjects.