

<i>Written by + date</i>	<i>Checked by + date</i>	<i>Approved by + date</i>	<i>Version</i>	<i>Page(s)</i>
Outi Nenonen and Armi Kaukoperko 26 September 2022	Outi Nenonen 26 September 2022	Juha-Pekka Jaskari 26 September 2022	3.1	1(2)

## **PRIVACY POLICY AT JPT SERCO OY**

The purpose of our privacy policy is to describe our operation which helps us secure data protection and enable related transparency for our clients, staff and other stakeholders. Our JPT Serco Oy staff and management are committed to complying with the EU General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, and the Data Protection Act (1050/2018).

Our privacy policy is reviewed and updated when necessary as part of our quality management system. In addition, we consider potential amendments in legislation and official guidelines. The regular review of the privacy policy is carried out by our Quality Manager in co-operation with the management.

### **1. Privacy policy documents and accessibility**

The privacy policy documents are the GDPR-compliant quality policy and the records, which correspond to privacy statements.

#### **We collect personal data and maintain them in the following records:**

- CLIENT ACCOUNT RECORD, in the production-management system
  - o Available at [www.serco.fi](http://www.serco.fi)
- SUPPLIER RECORD, in the production-management system
  - o Available at [www.serco.fi](http://www.serco.fi)
- SERCO NEWSLETTER SUBSCRIBER RECORD
  - o Available at [www.serco.fi](http://www.serco.fi)
- PAYROLL RECORD, personal details of JPT Jaskari employees in the payroll system
  - o Available in the production break room and by request from JPT Serco Oy Quality Manager.

Each register has its own record. These records describe the data in each register in detail as regards the following:

- data controller and name of record
- person responsible for the record
- purpose of record and regulatory legal basis
- data in the record
- data retention period
- regular data sources of record
- disclosure of data (e.g. outside ETA countries)
- how the data subject can apply their rights to the data
- principles of record protection

### **2. Acquiring, using and storing personal data**

We acquire the majority of personal data we use directly from our clients, suppliers, authorities, staff and other stakeholders. In addition, we benefit from existing client data as well as open corporate data on the internet. We use the personal data in our records to do business, manage customer relationships, and to inform and communicate about our activities.

We do not collect personal data beyond what is necessary for the above mentioned purposes. We store personal data in the records described above in such a format that permits identification of the data subject only for the duration of data processing.

<i>Written by + date</i>	<i>Checked by + date</i>	<i>Approved by + date</i>	<i>Version</i>	<i>Page(s)</i>
Outi Nenonen and Armi Kaukoperko 26 September 2022	Outi Nenonen 26 September 2022	Juha-Pekka Jaskari 26 September 2022	3.1	2(2)

### **3. Processing, protecting and deleting personal data**

We take data security and privacy requirements into account in the acquisition, development and maintenance of systems. Information systems and files containing personal data are protected by technical security measures that are standard in the business of our organisation. Access to these information systems and files requires a username and password. These are granted only to staff members of the systems and files administrator whose position and duties are connected with the access right in question. Our employees who process personal data are familiarised with the content of our privacy policy and are committed to complying with it. We also observe privacy policy in orientation training.

We update the personal data record continuously as soon as we have new data from data subjects or companies where they work or have worked. Inaccurate and mistaken data will be deleted or corrected without delay.

### **4. Procedure in case of data breach**

In case we suspect or detect a data breach, we immediately investigate it. We communicate it to relevant parties personally, if necessary, to correct the situation or restrict damage. We also notify the authorities of identified data protection issues as required by the GDPR.

### **5. Assessing risks of processing personal data**

We regularly (once a year) assess risks related to processing personal data as a part of our management quality review. The risk assessment always produces a separate document according to "JPT542LA\_Riskien hallinta" (risk management). The risk assessment and documentation of the results and measures are reported in a record: 'JPT5421LT\_Riskiraportti' (risk report).

We immediately take action to reduce significant risks related to processing personal data.

### **6. Transparency and rights of data subjects**

We want to operate in confidence towards the people who have given us their personal information i.e. the data subjects. This confidence also includes openness towards the data subjects and the rights of the data subjects.

The data subject has the right to:

- verify, rectify or access data that concerns them,
- request the restriction or erasure of data about them from our records if, for example, the personal data is no longer needed for the purpose for which it was originally stored,
- prohibit our company from processing data about them for direct marketing purposes,
- and to make other requests concerning the rights of the data subject by writing to one of our organisation's employees, whose contact details can be found on our website at [www.serco.fi](http://www.serco.fi).

At any time, the data subject has the right to withdraw their consent to process their personal data. Withdrawal of consent shall not affect the lawfulness of the processing carried out before the withdrawal, but it may prevent access to our products and services.