

11 May 2018

Privacy Notice for Customer Register

1 Controller

StatFinn, EPID Research
Metsänneidonkuja 12, 02130 Espoo
office@statfinn.com
(hereafter "we" or "COMPANY")

2 Contact person for register matters

Irina Panina
Paldiski mnt 29, 10612 Tallinn, Estonia
irina.panina@statfinn.com

3 Name of register

CUSTOMER REGISTER

4 What is the basis for and purpose of the processing of personal data?

The purpose of the processing of the personal data is managing our customer relationship matters and associated obligations, project management and coordination including IT system access and audit trail, where applicable, administration, invoicing, sales, marketing and contract activities.

None of the personal data we process under this register is subject to automatic decision-making or profiling that would have legal effects or impacts for the customer.

5 What data do we process?

We process the following personal data of our customers in connection with the customer register and to the extent necessary for the customer relationship activities:

- ✓ **Basic information of the customer company** such as company name, company bank account, company address;
- ✓ **Basic information of the customer representatives** such as firstname, lastname, work email, work phone number, company represented;
- ✓ **Information related to the customer representative relationship with the COMPANY** such as professional title and/or position, unit or function, qualifications and education;
- ✓ **Information related to content and documents that customer representative have created in the course of projects** such as protocols and other material;
- ✓ **Information of customer activity in the system (audit trail)** if customer is participating in the project documentation transfer through the COMPANY server;
- ✓ **Other possible information voluntarily given regarding the customer relationship between the controller and the customer.**

6 From where do we receive data?

We receive data primarily from the customer representative him-/herself. Secondly data may be received from public sources such as company website, business cards or personal contacts. In addition, audit trail data is received from the COMPANY IT systems used by the customer representative.

We process the data ourselves and engage subcontractors that process the data on behalf of and for us.

By entering into business relationship with the COMPANY, customer representative consents to the collection of data from his/her professional profiles to the extent such collection is necessary taking into consideration the nature of the business relationship.

7 To whom do we disclose data and do we transfer data outside of EU or EEA?

We disclose personal data in accordance with the applicable laws to a party, who based on law, collective bargaining agreement and/or agreement, has a right to receive information from the register. We also disclose data to the applicable COMPANY employees to perform their work duties.

We transfer personal data to subcontractors processing data on behalf of and for us. We use subcontractors in the processing of customers' personal data for the following services:

- Financial Administration and Invoice Management
- Legal Services
- IT and Telecom Systems
- Access Control and audit trail
- Project management and coordination

We have ensured your privacy with our subcontractors by entering into the necessary data processing agreements.

We may transfer low risk personal data outside of EU/EEA, including to the United States of America. We have taken care of suitable safeguards for the transfer, and use the EU Commission standard contractual clauses or another transfer mechanism approved by the privacy legislation.

8 How do we protect the data and how long do we store them?

Only those of our employees, who due to their working duties are entitled to process customer data, have the right to use systems containing customer data. Each user has a personal username and password to the systems. The information is collected into databases that are protected by firewalls, passwords, encryption and other technical measures. The databases and backup copies of them are stored in locked premises and can be accessed only by certain pre-designated persons. We also store paper copies of personal data in locked premises and the data may only be accessed by persons who are entitled to them due to their working duties.

We store the personal data for as long as is necessary for the purpose of the processing.

In addition, we take all reasonable actions to ensure that no incompatible, outdated or inaccurate personal data are stored in the register taking into account the purpose of the processing.