

Registry and Privacy Statement

The Foundation for the Baltic Institute is committed to complying with the [EU's General Data Protection Regulation \(GDPR\)](#), which applies in all EU member states as of 25 May 2018.

With this privacy statement, we inform individuals about the processing of their personal data. In order to be able to sign up for events organised by the Baltic Institute of Finland, a person must accept the terms of this privacy statement.

Last modified 20 January 2021

1. Data controller

The Foundation for the Baltic Institute
Kelloportinkatu 1, FI-33100 Tampere

2. Contact person responsible for the registry

Esa Kokkonen, esa.kokkonen@tampere.fi, +358 50 516 9111

3. Name of the registry

Registry of participants in the events organised by the Baltic Institute of Finland

4. Legal basis and purpose of processing personal data

The legal basis for processing personal data under the EU General Data Protection Regulation is the person's consent (documented, voluntary, identified, informed and unambiguous).

The data will not be used for automated decision-making or profiling, nor will it be disclosed to third parties.

The personal data collected is used for

- collecting event registrations
- communication with people registered for the events
- for collecting feedback on the events

5. Data content of the registry

The participant registry for the events organised by the Baltic Institute of Finland contains the following information related to a natural person:

- name
- email

- phone number
- title
- company or organisation to which the person is associated
- special diet
- other necessary information depending on the event, e.g. whether or not the participants attends lunch

6. Regular sources of information

The data source is the user him or herself. At the user's request, all personal data concerning him or her may be deleted from the registry of the Baltic Institute of Finland.

We will only retain personal information as long as necessary to fulfill the purposes described above. As a rule, the data of the event registrees is deleted from the registry one month after the event.

7. Regular data release and transfer of data outside the EU or the EEA

The data is not regularly disclosed to other parties. The information may only be published to the extent agreed with the user .

Data may be transferred to the following software:

Google Forms Questionnaires – Google is a part of the EU-US Privacy Shield Framework.

8. Registry security principles

The registry shall be handled with due care, and the data processed by information systems shall be adequately protected. When registry information is stored on internet servers, the physical and digital security of the hardware is taken care of accordingly. The controller shall ensure that the data stored, as well as the access rights to the servers and other information critical to the security of personal data, are treated confidentially and only by the employees whose job description requires it.

9. Right to inspect data and to request correction of information

Every person listed has the right to check the information stored in the registry and to request the correction of any false information or the amendment of incomplete information. If a person wishes to check the data stored about him or her or request a correction, the request must be sent in writing to the data controller. If necessary, the controller may ask the applicant to prove his or her identity. The controller will respond to the customer within the timeframe set out in the EU Data Protection Regulation (generally within one month).

10. Other rights related to processing of personal data

A person in the registry has the right to request the removal of his or her personal data (i.e. "the right to be forgotten"). Data subjects also have other rights under the EU's general data protection regulation, such as restrictions on the processing of personal data in certain situations. Requests must be sent in writing to the controller. If necessary, the controller may ask the applicant to prove his or her identity. The controller will

respond to the customer within the timeframe set out in the EU Data Protection Regulation (generally within one month).