RAKENNUSTIETO

1.5.2024

Privacy Policy Annex

1. General information

This annex regarding the processing of personal data and data protection ("Privacy Policy Annex") is an integral and essential part of the General Contract Terms and Terms of Use ("Terms and conditions") of Rakennustieto Ltd ("Rakennustieto"), the up-to-date version of which is available at https://www.rakennustieto.fi/yleiset-sopimusehdot.

This Privacy Policy Annex applies when Rakennustieto establishes a customer relationship with its customer ("Customer") and thereby processes the Customer's personal data in accordance with the EU General Data Protection Regulation (2016/67) ("GDPR"), either for its own purposes or on behalf of and for the account of the Customer.

This Privacy Policy Annex, together with the agreement between Rakennustieto and the Customer ("Agreement") sets out the principles and conditions of data protection and security of personal data. In the event of any conflict between the Agreement and its other possible annexes and this Privacy Policy Annex, the processing of personal data between Rakennustieto and the Customer shall be governed primarily by this Privacy Policy Annex.

2. Definitions

"Personal data" means any information relating to an identified or identifiable natural person ("Data Subject") or other personal data as defined in the GDPR or other data protection legislation.

"Processing" means any operation or set of operations that is performed on personal data or on sets of data containing personal data, whether by automatic or manual means, or any other processing of personal data as defined in the GDPR or other data protection legislation.

"Controller" means, for the purposes of the GDPR, the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" means, for the purposes of the GDPR, the entity which processes personal data on behalf of the Controller.

"Personal data breach" means an event that results in the destruction, loss, alteration, unauthorized disclosure or access to personal data by an unauthorized party.

3. Roles

Rakennustieto acts as the Controller within the meaning of the GDPR when it processes the Customer's personal data for its own purposes so that these personal data form the Customer Register of Rakennustieto.

When Rakennustieto processes personal data on behalf of the Customer and for the account of the Customer, the Customer acts as the Controller and Rakennustieto as the Processor. Thus, Rakennustieto acts as a Processor when processing personal data that the Customer has added to the Service of Rakennustieto.

4. Rights and obligations of the Controller

The Controller is responsible for the definition of the personal data to be processed and for ensuring that it processes personal data in accordance with the GDPR and other data protection legislation and good data processing practices. The Controller is responsible for ensuring that there is a legal basis for the processing of personal data in accordance with the GDPR.

The Controller is obliged to define the purposes and means of the processing of personal data and to provide the Processor with binding written instructions on the processing of personal data in accordance with the GDPR.

The Controller shall ensure and be responsible for providing the Data Subject with all information required by the GDPR regarding the processing of personal data. In addition, the Controller shall be responsible for ensuring that, throughout the term of the Agreement, it has the right under the GDPR to transfer personal data for processing in accordance with this Privacy Policy Annex and the Agreement.

The Controller is responsible for obtaining the necessary consent for the processing of personal data. In addition, the Controller is responsible for complying with all mandatory notification and authorization obligations and requirements to the authorities in relation to the processing of personal data. The Controller is responsible for implementing its own requests for amendment, deletion and in formation to its stakeholders in accordance with the GDPR.

The Controller is responsible for what data is stored in the service, how it is processed (including possible pseudonymization) and where it is disclosed to. The Controller is solely responsible for the accuracy, timeliness, content, reliability and lawfulness of the personal data provided to the Processor.

Both the Controller and the Processor shall be liable for any costs incurred by them in fulfilling their respective obligations under the GDPR or other data protection legislation or this Privacy Policy Annex.

5. Rights and obligations of the Processor

The Processor shall act in accordance with this Privacy Policy Annex when providing services to the Controller under the Agreement. The Processor shall only use personal data for the purposes of fulfilling its obligations under the Agreement.

The Processor shall comply with the applicable data protection legislation and the written instructions provided by the Controller. The Processor is obliged to inform the Controller immediately if it considers the instructions to be unlawful, unless such information would be prohibited by law for important reasons of public interest.

The Processor shall ensure that those who have access to the personal data are aware that they are only entitled to process personal data in accordance with the Controller’s

instructions, this Privacy Policy Annex and the GDPR and other applicable data protection legislation. The Processor undertakes to ensure that all persons under its authority who are entitled to process personal data are bound by the obligation of professional secrecy or are subject to an appropriate legal obligation of secrecy.

In addition to the requirements on the protection of personal data, data security and confidentiality set out in the Agreement, the Processor undertakes to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in order to ensure the security of the processing of personal data, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing and risks to the rights and freedoms of natural persons, which vary in terms of likelihood and severity, and to comply with the instructions of the Controller. The Processor shall ensure at least the following measures: pseudonymization and encryption of personal data to the extent required by the Controller; the possibility to ensure at all times the confidentiality, integrity, availability and sustainability of the systems and services used for the processing of personal data; the availability of personal data and the restoration of access to personal data without delay following a physical or technical breakdown.

The Processor undertakes to inform the Controller without undue delay of any request received from Data Subjects concerning the exercise of their rights under the GDPR and other data protection legislation.

The Processor is obliged to assist the Controller in activities where the Controller needs the Processor's cooperation in order to fulfill its obligations under the GDPR. Such activities may include, for example, participating in impact assessments and providing data protection-related habits and reports. If the Controller requests information or assistance on data security measures, documentation or other information related to the Processor's processing of personal data in a way that the requests differ in substance from the GDPR or other applicable data protection legislation and this results in additional work for the Processor, the Processor shall be entitled to charge the Controller for such additional services.

As stated above, the Controller and the Processor shall be responsible for their own costs incurred in fulfilling their respective obligations under the GDPR or this Privacy Policy Annex.

The Processor has no control over what information the Controller stores on the service, but the security practices are designed to allow the Controller to have personal data in the service of the Processor.

6. Use of subcontractors and transfer of data

The Processor may use subcontractors to provide services to the Controller in accordance with this Privacy Policy Annex. The Processor shall ensure that its subcontractor complies with the confidentiality, security and data protection requirements of this Privacy Policy Annex and the Agreement, as well as the GDPR and other data protection legislation.

The Processor shall have the right to change subcontractors during the term of the Agreement. The Processor shall inform the Controller in advance of any changes in the subcontractors' processing of personal data.

The Processor shall not transfer personal data outside the EU or EEA unless it follows the procedure set out in this paragraph. The transfer of personal data to third countries may be carried out by means of an appropriate transfer agreement in accordance with the EU Commission's standard contractual clauses and/or other applicable requirements for the transfer of personal data in force at the time.

7. Duration of processing and deletion of data

The Processor will process personal data only for as long as the Agreement is in force.

Upon the termination of the Agreement, the Processor shall, at the choice of the Controller, either permanently erase the personal data or return all personal data to the Controller and, in addition, erase any existing copies, except where the law requires the retention of personal data for a specified period after the termination of the Agreement.

8. Handling data breaches

The Processor shall notify the Controller of any data breach without undue delay and, where possible, within 72 hours of becoming aware of the data breach. The notification shall include the following information:

- a description of the breach, including which categories of Data Subjects were affected by the breach and the estimated number of such categories;
- the name and contact details of the contact person of the processor in charge of investigating the breach;
- a description of the actual and/or likely consequences of the breach; and
- a description of the measures taken by the processor to respond to the breach and to mitigate its adverse effects.

If it is not possible to provide the above information at the same time, the information may be provided in parts.

The Controller shall inform the Processor without undue delay if the Controller suspects a data breach. The Controller is also obliged to assist in the investigation of the breach and to provide the processor with the information necessary to investigate the breach. The Processor has the right to suspend the investigation of a data breach if the Controller does not respond to the contacts or if the interest to be protected is manifestly negligible.

In the event of a possible data breach, the Controller will be informed by the Processor and the Controller is responsible for passing on the information.

9. Liability and other terms

If the Data Subject suffers damage as a result of a breach of data protection obligations, the Controller and the Processor shall be liable for the damage suffered by the Data Subject in accordance with Article 82 of the GDPR. The Controller and the Processor shall each be liable for any sanctions imposed on them by the competent supervisory authority.

This Privacy Policy Annex shall remain in force as long as the Agreement is in force and for as long as necessary to complete the activities related to the processing of personal data (such as the return of personal data to the Controller) after the termination of the Agreements or the expiry of the Agreement period, or longer if applicable law so provides.

Obligations which, by their nature, are intended to survive the expiry of this Annex, shall survive the expiry of this Annex.

The Annex shall be governed by the laws set forth herein and any disputes shall be resolved in accordance with the provisions of the Agreement.