Personal Data Processing Agreement

Document version: v2.2

Valid from /2024-03-01

Table of Contents

1. INTRODUCTION

The main activity of UAB iSense Technologies is development, implementation and maintenance of information systems for public sector organisations and business companies.

1.1. Overview of the document

This agreement regarding the processing of personal data is entered into by and between UAB iSense Technologies, legal entity code 302553999 (hereinafter referred to as the Service Provider) and the Customer, hereinafter collectively referred to in this Agreement as the Parties or each individually as a Party, whereas:

- The Parties shall enter into a service contract on the basis of which the Data Processor provides services to the Data Controller (hereinafter referred to as the Contract);
- On the basis of the Contract, the Data Processor shall process, on behalf of the Data Controller, the personal data of the relevant data subjects provided by the Data Controller;
- The Parties intend that the Contract shall be performed in compliance with the requirements for the protection of personal data and have therefore entered into this Personal Data Processing Agreement (hereinafter referred to as the Agreement) in connection with the Contract on the terms and conditions set out below.

1.2. Amendments to the Document

Version	Date	Description
1.1	25/06/2023	Initial version of the document
1.2.2	29/06/2023	Working version of the document
2.2	01/12/2023	Version for coordination with RRT

1.3. Terms and abbreviations used

Abbreviations	Description
Personal Data	personal data (excluding special categories of personal data) as defined in Article 4(1) of the Regulation, which the Data Controller makes

	available to the Data Processor and/or allows access to, in accordance with the terms of this Agreement;
Personal Data Subject	a natural person whose Personal Data is processed in accordance with the Regulation, other legal acts regulating the legal protection of personal data, and the terms of this Agreement;
Data processing	any operation or set of operations which is performed upon personal data, whether or not by automated means, including, but not limited to: collection, recording, classification, organisation, storage, adaptation or alteration, retrieval, access, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination with other data, restriction, erasure or destruction;
Regulation or GDPR	shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
Incident	An event or set of circumstances occurring in the information technology infrastructure managed by the Data Controller which causes a disruption to the services or systems provided by the Data Processor;
Personal Data Breach	an event or set of circumstances which may result in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
Responsible Person of the Data Controller	a responsible person appointed by the Data Controller (administrator or security officer) intended to coordinate incident resolution and control access rights to data stored in the Data Controller's IS;

Other terms in the Agreement shall have the meanings as defined in the Contract and in the personal data protection legislation.

2. PURPOSE, NATURE OF DATA PROCESSING

Subject-matter and purpose of processing: for the purpose of the performance of the Contract, personal data and/or sets of personal data processed by the Data Controller, with which the Data

Processor needs to carry out processing operations by automated means, shall be transmitted to the Data Processor.

3. DURATION OF DATA PROCESSING

This Agreement shall apply for as long as the Data Processor processes personal data on behalf of the Data Controller in accordance with the Contract and this Agreement.

4. OBLIGATIONS OF THE DATA PROCESSOR

- The Data Processor undertakes to process only the personal data referred to in this Agreement and for the purposes set out in the Agreement, and in accordance with the personal data protection legislation, the Regulation and the documented instructions of the Data Controller.
- The Data Processor shall appoint a Data Protection Officer who shall ensure the proper performance of the tasks referred to in Article 39 of the GDPR.
- The Data Processor shall, during the term of the Agreement, implement appropriate technical and organisational measures to ensure that the processing of personal data carried out by it in accordance with the provisions of this Agreement complies with the requirements of the applicable data protection legislation, in particular with the requirements of the GDPR, and to guarantee the protection of the rights of the data subject. A description of the technical and organisational measures used by the Data Processor at the time of the conclusion of the Contract and this Agreement shall be set out in Annex 1.
- The Data Processor shall, taking into account the nature of the processing and to the extent possible through the use of appropriate technical and organisational means, assist the Data Controller in fulfilling the Data Controller's obligation to respond to requests for the exercise of the rights of the data subject. Under this Agreement, the data subject's rights shall include the rights to request information and, at the data subject's request, to rectify, erase or suspend processing of personal data.
- The Data Processor shall, taking into account the nature of the processing and the information available to it, assist the Data Controller in complying with its specific obligations under applicable data protection legislation. Specific obligations shall include security of data processing (Article 32 of the

GDPR), notification of a personal data breach (Articles 33–34 of the GDPR) and data protection impact assessment as well as prior consultation (Articles 35–36 of the GDPR).

- The Data Processor undertakes to provide the Data Controller with all information and assistance necessary to demonstrate compliance with its obligations under this Agreement, and to facilitate and assist audits, including on-the-spot verifications, by the Data Controller or any other auditor authorised by the Data Controller.
- The Data Controller may carry out a more detailed audit at its own expense, which shall be:
  - limited to matters specifically related to the Data Controller and agreed upon in advance with the Data Processor;
  - carried out with a reasonable period of notice, which may not be less than 4 weeks, unless there are identifiable substantial obstacles;
  - performed in such a way as not to interfere with the daily activities of the Data Processor.

5. SUB-PROCESSORS

- The Data Processor shall have the right to engage another data processor. The Data Processor shall ensure that the person it engages complies with the requirements of the personal data protection legislation (including the implementation of appropriate organisational and technical measures) and with the obligations imposed on the Data Processor by this Agreement to the same extent as the Data Processor itself, and shall be liable to the Data Controller for the performance of the obligations of the third party engaged.
- The Data Processor shall ensure and, at the request of the Datat Controller, document that the sub-processors are bound by written contracts which, in addition to the obligations set out in this Agreement, oblige them to perform the relevant data processing obligations. The Data Processor shall be fully liable to the Data Controller for the performance of the obligations of the sub-processors.

6. TRANSFER OF DATA TO THIRD COUNTRIES

The obligation to process personal data under the Agreement may only be performed in a Member State of the European Union (EU) or a Member State of the European Economic Area (EEA).

Any transfer of personal data to a country that is not a Member State of the EU or EEA may only take place with the prior written consent of the Data Controller and only if the specific conditions set out in the applicable data protection legislation, Chapter V of the GDPR, are met.

7. INFORMATION SECURITY AND CONFIDENTIALITY

- The Data Processor shall ensure adequate protection of personal data in accordance with this Agreement for the purpose of protecting personal data against destruction, alteration, unauthorised dissemination or access. Personal data shall also be protected against any other unlawful processing.
- The Data Processor shall draw up and keep up-to-date a description of its technical, organisational and physical measures to comply with the requirements of the applicable data protection legislation. A checklist of the measures to be used shall be provided in Annex 1.
- The Data Processor undertakes not to disclose or otherwise make available to any third party, other than the sub-processors engaged under this Agreement, any personal data processed under this Agreement, without the prior written consent of the Data Controller.
- The Data Processor shall ensure that all persons involved in the processing of personal data are permanently bound by a non-disclosure agreement or are subject to an appropriate statutory obligation of confidentiality.
- If for any reason either Party is unable to comply with the terms and conditions of this Agreement, it shall immediately notify the other Party.

8. PERSONAL DATA BREACHES

- In the event of a Personal Data Breach or where the Data Processor has reasonable grounds to suspect a Personal Data Breach, the Data Processor shall, without delay and in any event not later than 24 hours after becoming aware of the breach, inform the Data Controller in writing of the breach and shall provide the Data Controller with the information and data in its possession in relation to such breach.
- At the request of the Data Controller, the Data Processor shall, without undue delay and subject to technical feasibility, provide the Data Controller with the additional requested documents, information and the data necessary to enable the Data Controller to establish and/or verify the fact of

the Personal Data Breach, to investigate its circumstances and to take immediate measures to eliminate the breach or to mitigate its negative consequences.

9. LIABILITY OF THE DATA PROCESSOR, DISPUTE RESOLUTION PROCEDURE AND CONTACT PERSONS

- Taking into account the nature, scope, context and purposes of the processing of Personal Data, including the fact that the Data Processor is obliged to process Personal Data as an integral condition for the proper implementation of the Agreement, the Parties consider that in the event of a violation of the Agreement/misperformance of the Agreement, or a violation of the Regulation, the Data Processor shall compensate for the damage caused.
- The Parties shall not be liable for operating losses, loss of profits, loss of goodwill and any other indirect losses and consequential damages.

Annex 1

Checklist of Technical and Organisational Security Measures Used by the Data Processor

Name of the measure	Description of the use of the measure
Risk management (regular inspection, evaluation and assessment of effectiveness)	• Regular analysis of the tangible and intangible losses that may arise in the course of data processing activities and in the underlying data processing systems; • Information security risk assessment (ISO 27005) and compliance assessment carried out once a year.
Access control	• Physical security concept that defines security zones (public areas, office, data centre); • Access is controlled by access permissions; • Access to the data centre is protected by advanced security measures; • Access to personal data is granted through a secure registration process and a secure password policy (strong passwords, regular password changes; • Procedure for confirming and revoking access permissions is in place, and passwords are transmitted securely; • Access permissions are regularly checked and updated; • External access to personal data is only possible using encryption methods (SSL and/or VPN).
Control of the information network	• A firewall is used to securely isolate information systems from external access from public networks; • The use of anti-virus software is checked regularly; • Relevant security updates are regularly imported.
Transmission control	• Remote access (over public networks) is always encrypted; • Specifications and processes for the physical destruction of documents are established.
Retention control	• Rules on the retention of personal data are established; • Access to personal data is provided based on assigned personal user accounts; • Data transfer log files/protocols are used.

Control of instructions	• There are defined responsibilities (e.g. data owner, system maintainer) for the tasks of data processing and related systems; • There is a clear regulation of the responsibilities for data processing (data controller <-> data processor, sub-processor, etc.); • Employees are trained on data protection issues and awareness-raising measures are in place; • Data Processor employees are required to comply with a separate non-disclosure agreement; • The sub-processors having access to the data controller's data must comply with all the technical and organisational measures included in this checklist.
Control of accessibility	• Physical security measures are in place to protect access to personal data (fire protection measures, air conditioning, UPS protection); • Data backups are carried out regularly; • Backups are stored in an external repository or secure alternative environment; • Systems are automatically monitored at all times; • Reporting of IT incidents and measures taken to resolve system performance problems; • Measures are in place to identify potential data protection incidents.
Separation control	• Production and testing systems are separated; • The Data Processor's employees have been instructed that personal data may only be processed for the purposes intended.