

# Data Processing Agreement

The following agreement is a supplement to Lantero's general service agreement pursuant to Article 28.3 of the General Data Protection Regulation EU 2016/679.

## 1 PARTIES, POSITIONS OF THE PARTIES, CONTACT DETAILS AND CONTACT

Parties and contact persons according to service agreements. The customer is the Personal Data Controller and Lantero the Personal Data Processor.

## 2 DEFINITIONS

2.1 In addition to the concepts defined in the text for the Data Processing Agreement, these definitions shall, regardless of whether they are used in the plural or singular, in definite or indefinite form, have the following meaning when entered with capital letters as the initial letter.

### Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### Data protection legislation

Refers to all privacy and personal data legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this Agreement, including national legislation and EU legislation.

### Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

### Instruction

The written instructions that more specifically define the object, duration, type and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing.

### Log

A Log is the result of Logging

### Logging

Logging is a continuous collection of information about the Processing of Personal Data that is performed according to this Agreement and which can be associated with an individual natural person.

Processor

A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

Personal Data

Any information relating to an identified or identifiable natural person, where an identifiable natural person is a person who directly or indirectly can be identified in particular by reference to an identifier such as name, social security number, location data or online identifiers or one or more factors which are specific to the natural person's physical, physiological, genetic, psychological, economic, cultural or social identity.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Data Subject

Natural person whose Personal Data are Processed.

Third Country

A state that is not a member of the European Union (EU) or the European Economic Area (EEA).

Subprocessor

A natural or legal person, public authority, agency or other body which, in the capacity of subcontractor to the Processor, Processes Personal Data on behalf of the Controller.

### **3 BACKGROUND AND AIM**

- 3.1 Through this Agreement, the Instructions and a list of possible Subprocessors (hereafter jointly referred to as “the Agreement”), the Controller regulates Processor’s Processing of Personal Data on behalf of the Controller. The aim of the Agreement is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with what is stipulated in Article 28(3) of the General Data Protection Regulation (EU) 2016/679 (“GDPR”).
- 3.2 If anything stipulated in item 1, paragraph 3.2, item 165 or 16, paragraph 18.6, items 19–20 or 23 in this Agreement is otherwise regulated in the Main Agreement, the regulation of the Main Agreement shall have precedence.
- 3.3 References in this Agreement to national or EU legislation refer to applicable regulations at any given time.

## 4 PROCESSING OF PERSONAL DATA AND SPECIFICATION

- 4.1 The Controller hereby appoints the Processor to carry out the Processing on behalf of the Controller in accordance with this Agreement.
- 4.2 The Controller shall give written instructions to the Processor on how the Processing should be carried out.
- 4.3 The Processor may only carry out the Processing pertaining to this Agreement and the instructions in force at any given time.

## 5 OBLIGATIONS OF THE CONTROLLER

- 5.1 The Controller undertakes to ensure that there is a legal basis for the Processing at all times and for compiling correct Instructions with regard to the nature of the Processing so that the Processor and any Subprocessor can fulfill their tasks according to this Agreement and Main Agreement, where applicable.-
- 5.2 The Controller shall, without unnecessary delay, inform the Processor of changes in the Processing which affect the Processor's obligations pursuant to Data Protection Legislation.
- 5.3 The Controller is responsible for informing Data Subjects about the Processing and protecting the rights of Data Subjects according to Data Protection Legislation as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

## 6 OBLIGATIONS OF THE PROCESSOR

- 6.1 The Processor undertakes to only perform the Processing in accordance with this Agreement and for the specific purposes stipulated in the Instructions, as well as to comply with Data Protection Legislation. The Processor also undertakes to continuously remain informed about applicable law in this area.
- 6.2 The Processor shall take measures to protect the Personal Data against all types of Processing which are incompatible with this Agreement, Instructions and Data Protection Legislation.
- 6.3 The Processor undertakes to ensure that all natural persons working under its management follow this Agreement and Instructions and that such natural persons are informed of relevant legislation.
- 6.4 The Processor shall, at the request of the Controller, assist in ensuring that the obligations pertaining to Articles 32-36 in the GDPR are fulfilled and respond to requests for the exercise of a Data Subject's rights pertaining to the GDPR, Chapter III, taking into account the type of Processing and the information which the Processor has access to.
- 6.5 In the event that the Processor finds the Instructions to be unclear, in violation of the Data Protection Legislation or non-existent, and the Processor is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, the Processor shall

inform the Controller of this without delay, temporarily suspend the Processing and await new Instructions, if the Parties have not agreed otherwise.

- 6.6 If the Controller provides the Processor with new or revised Instructions, the Processor shall without unnecessary delay from receipt, communicate to the Controller whether the implementation of the new Instructions causes changed costs for the Processor.

## **7 SECURITY MEASURES**

- 7.1 The Processor shall take all appropriate technical and organizational security measures required pertaining to Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the procedure of Processing meets the requirements of the GDPR and that the rights of the Data Subjects are protected.
- 7.2 The Processor shall continuously ensure that the technical and organizational security in connection with Processing is executed with an appropriate level of confidentiality, integrity, accessibility and resilience.
- 7.3 Any added or revised requirements for protective measures from the Data Controller, after the Parties have signed this Agreement, will be considered as new Instructions pertaining to this Agreement.
- 7.4 The Processor shall, through its control systems for authority, only grant access to the Personal Data for such natural persons working under the Processor's management and who need access to be able to perform their duties.
- 7.5 The Processor undertakes to continuously log access to the Personal Data in accordance with this Agreement to the extent required according to the Instructions. Logs may be erased only five (5) years after the logging event, unless otherwise stated in the Instructions. Logs will be subject to the required protection measures pertaining to Data Protection Legislation.
- 7.6 The Processor shall systematically test, investigate and evaluate the effectiveness of the technical and organizational measures which will ensure the security of the Processing.

## **8 SECRECY/DUTY OF CONFIDENTIALITY**

- 8.1 The Processor and all natural persons working under its management shall observe both confidentiality and professional secrecy during the Processing. The Personal Data may not be used or disseminated for other purposes, either directly or indirectly, unless otherwise agreed.
- 8.2 The Processor shall ensure that all natural persons working under its management, participating in the Processing, are bound by a confidentiality agreement pertaining to the Processing. However, this is not a requirement if they are already covered by a legally sanctioned duty of confidentiality. The Processor also undertakes to ensure that there is a nondisclosure agreement with its Subprocessor and confidentiality agreement between the Subprocessor and all natural persons working under its management, participating in the Processing.

- 8.3 The Processor shall promptly inform the Controller of any contacts with supervisory authorities pertaining to the Processing. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards supervisory authorities in matters relating to the Processing.
- 8.4 If the Data Subject, supervisory authority or third Party requests information from the Processor pertaining to the Processing, the Processor shall inform the Controller about the matter. Information about the Processing may not be submitted to the Data Subject, supervisory authority or third parties without written consent from the Controller, unless mandatory law so stipulates that such information must be provided. The Processor shall assist with the communication of the information covered by a consent or legal requirement.

## 9 INSPECTION, SUPERVISION AND AUDITING

- 9.1 The Processor shall, without unnecessary delay, as part of its guarantees, pursuant to Article 28.1 of the GDPR, be able to report, at the request of the Controller, which technical and organisational security measures are being used for the processing to meet the requirements according to the DPA and Article 28.3.h of the GDPR.
- 9.2 The Processor shall review the security of the Processing at least once a year by performing a checks to ensure that the Processing complies with this Agreement. Upon request, the results of such checks shall be shared with the Controller.
- 9.3 The Controller or a third party it appoints (who cannot be a competitor of the Processor) is entitled to check that the Processor meets the requirements of this Agreement, Instructions and Data Protection Legislation. During such a check, the Controller shall assist the Controller, or the person carrying out the review on behalf of the Controller, with documentation, access to premises, IT systems and other assets needed to be able to check the compliance of the Controller with this Agreement, Instructions and Data Protection Legislation. The Controller shall ensure that staff who carry out the check are subject to confidentiality or non-disclosure obligations pertaining to law or agreement.
- 9.4 As an alternative to the stipulations of items 9.2–9.3, the Processor is entitled to offer other means of checking the Processing, such as checks carried out by independent third parties. In such a case, the Controller shall have the right, but not the obligation, to apply such alternative means. In the event of such a check, the Processor shall provide the Controller or third party with the assistance needed for performing the check.
- 9.5 The Processor shall provide the supervisory authority, or other authority which has the legal right to do so, the means to carry out supervision according to the authority's request pertaining to the legislation in force at any time, even if such supervision would otherwise be in conflict with the provisions of this Agreement.
- 9.6 The Processor shall assure the Controller rights towards any Subprocessor corresponding to all of the rights of the Controller towards the Processor according to section 9 of this Agreement.

- 9.7 The Personal Data Processor has the right to invoice the Customer for any costs that may arise in connection with 9.1, 9.3 and 9.4.

## 10 HANDLING OF CORRECTIONS AND DELETIONS ETC

- 10.1 In the case of the Controller requesting correction or deletion due to incorrect processing by the Processor, the Controller shall take appropriate action without unnecessary delay, within thirty (30) days at the latest, from the time the Processor has received the required information from the Controller. When the Controller requests deletion, the Processor may only carry out Processing of the Personal Data in question as part of the process for correction or deletion.
- 10.2 If technical and organizational measures (e.g., upgrades or troubleshooting) are taken by the Processor in the Processing, which can have an effect on the Processing, the Processor shall inform the Controller in writing pursuant to what is stipulated about notifications in item 19 of this Agreement. The information shall be submitted in good time prior to the measures being taken.

## 11 PERSONAL DATA BREACHES

- 11.1 The Processor shall have the capability to restore accessibility and access to Personal Data within a reasonable time in the event of a physical or technical incident pertaining to Article 32.1.c of the GDPR.
- 11.2 The Personal Data Processor undertakes, taking into account the nature of the Processing, and the information available to the Personal Data Processor, to assist the Personal Data Administrator in fulfilling its obligations in the event of a Personal Data Breach regarding the Processing. The Personal Data Processor shall, at the request of the Personal Data Controller, also assist in investigating suspicions of possible unauthorized persons' Processing and/or access to the Personal Data.
- 11.3 In the event of a Personal Data Breach, which the Processor has been made aware of, the Processor shall notify the Controller of the Breach in writing without unnecessary delay. The Processor shall, taking into account the type of Processing and the information available to the Processor, provide the Controller with a written description of the Personal Data Breach.

The description shall give an account of:

- a. The nature of the Personal Data Breach and, if possible, the categories and number of Data Subjects affected and the categories and number of Personal Data records affected,
  - b. the likely impact of the Personal Data Breach, and
  - c. measures taken or proposed and measures to mitigate the potential negative effects of the Personal Data Breach.
- 11.5 If it is not possible for the Processor to provide the full description at the same time, according to item 11.3 of this Agreement, the description may be provided in installments without unnecessary further delay.

## 12 SUBPROCESSOR

- 12.1 The Processor has the right to engage the Subprocessor or Subprocessors who are necessary to deliver the service in accordance with the Main Agreement. The Controller may at any time request a written report of the relevant Subprocessors.
- 12.2 The Processor undertakes to sign a written agreement with a Subprocessor regulating the Processing which the Subprocessor carries out on behalf of the Controller and to only employ Subprocessors who provide sufficient guarantees. Subprocessors shall take all appropriate technical and organisational measures so that the Processing meets the requirements of Data Protection Legislation. Regarding data protection, the agreement shall impose the same obligations on a Subprocessor as are imposed on the Processor under this Agreement.
- 12.3 The Processor is fully responsible for the Subprocessor's Processing towards the Personal Data Controller.
- 12.4 The Processor is entitled to employ new Subprocessors and replace existing Subprocessors.
- 12.5 When the Processor intends to hire a new or replace an existing Subprocessor, the Processor shall ensure the capacity and capability of the Subprocessor to fulfil its obligations pursuant to Data Protection Legislation.
- 12.6 The Processor shall, at the request of the Controller, submit a copy of the Agreement regulating the Personal Data Processing by a Subprocessor and the list of Subprocessors pursuant to item 12.2.

## 13 LOCATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

- 13.1 The Processor shall ensure that the Personal Data shall be handled and stored within the EU/EEA by a natural or legal person who is established in the EU/EEA, unless the parties to this Agreement agree otherwise.
- 13.2 The Processor is only entitled to transfer Personal Data to a Third Country for Processing (e.g. for service, support, maintenance, development, operations or other similar handling) if the Controller has given advance written approval of such transfer and has issued Instructions to this end.
- 13.3 Transfer to a Third Country for Processing in accordance with item 13.2 of the Agreement may be carried out only if it complies with the Data Protection Legislation and fulfils the requirements for the Processing set out in this Agreement and the Instructions

## 14 LIABILITY FOR DAMAGE IN CONNECTION WITH THE PROCESSING

- 14.1 In the event of a compensation for damage in connection with Processing, through a judgment given or settlement, to be paid to a Data Subject due to an infringement of a provision in the Agreement, Instructions and/or applicable provision in Data Protection Legislation, Article 82 of the GDPR shall apply.

- 14.2 Fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Data Protection Act (2018:218) with supplementary provisions to the EU's data protection regulation shall be borne by the Party to the Agreement named as recipient of such sanctions.
- 14.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimize the damage or loss.
- 14.4 Regardless of the content of the Main Agreement, items 14.1 and 14.2 of this Agreement take precedence to other rules on the distribution between the Parties of claims among themselves as far as the processing is concerned.

## **15 CHOICE OF LAW AND DISPUTE RESOLUTION**

- 15.1 This agreement is governed by Swedish law. Any interpretation or dispute in connection with the PUB agreement, which the parties cannot resolve on their own, shall be decided by a Swedish general court.

## **16 CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT**

- 15.1 This Agreement shall enter into force from the time the Agreement is signed by both Parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days' notice.

## **17 AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECT, ETC.**

- 17.1 Each party to the Agreement shall be entitled to invoke a renegotiation of the Agreement if there is a major change of the ownership of the other party or if applicable legislation or interpretation thereof changes in a way that significantly affects the Processing. The invoking of a renegotiation pursuant to the first sentence does not mean that any part of the Agreement will cease to be in effect, but only means that a renegotiation of the Agreement will commence.
- 17.2 Additions and amendments to the Agreement must be made in writing and signed by both parties.
- 17.3 If either party becomes aware that the other party is acting in violation of the Agreement and/or Instructions, the first party shall inform the other party without delay of the actions in question. The party is then entitled to suspend the performance of its obligations pursuant to the Agreement until such time as the other party has declared that the actions have ceased, and the explanation has been accepted by the party that made the complaint.
- 17.4 If the Controller objects to the Processor using a new Subprocessor, pursuant to item 12.6 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.

## **18 MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT**



- 18.1 Upon termination of the Agreement, the Processor shall, without unnecessary delay, depending on what the Controller chooses, either delete and certify to the Controller that it has been carried out, or return
- a. all Personal Data Processed on behalf of the Controller and
  - b. all associated information such as Logs, Instructions, system solutions, descriptions and other documents which the Processor has obtained through information exchange in pursuance of the Agreement.
- 18.2 Delivery and deletion in accordance with the Agreement, section 18.1, shall be completed no later than thirty (30) days from the date of termination under this Agreement, section 16.1.
- 18.3 Processing carried out by the Personal Data Processor after the date stipulated in section 18.2 is to be regarded as an unlawful Processing.
- 18.4 The provisions on confidentiality/professional secrecy in section 8 under this Agreement shall continue to apply even if the Agreement otherwise ceases to apply.

## **19 NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND THE INSTRUCTIONS**

- 19.1 Notifications about the Agreement and its administration, including termination, shall be submitted to each Party's contact person for the Agreement.
- 19.2 Notifications about the collaboration of the Parties regarding the data protection shall be submitted to each Party's contact for the Parties' cooperation on data protection.
- 19.3 A notification shall be deemed to have reached the recipient no later than one (1) business day after the notification has been sent.

## **20 CONTACT PERSONS**

- 20.1 Each Party shall appoint their contact person for the Agreement, which is the contact person specified when purchasing the service, unless otherwise specifically stated.
- 20.2 Each Party shall appoint their contact person for the Parties' cooperation on data protection, which is the contact person specified when purchasing the service, unless otherwise specifically stated.

## **21 RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION**

- 21.1 Each Party is responsible for the information entered in item 1 of the Agreement always being current and correct. Change of information in item 1 shall be communicated to the other Party pursuant to item 19.1 of the Agreement.

## 22 INSTRUCTIONS FOR HANDLING PERSONAL DATA

22.1 Personal data processing within the framework of the whistleblowing service shall take place in accordance with the following instructions.

### Purpose of processing personal data

The whistleblowing function is a reporting channel that aims to enable whistleblowers to report serious misconduct. The processing takes place in order to administer the receipt of whistleblower reports, enable correspondence between the whistleblower and the investigator and to hand over reports to the controller or to an external investigator.

### Categories of personal data that may be processed by the processor

The Personal Data Processor may have access to Personal Data about users in the system and about individuals affected by a reported case. Types of personal data can be, for example:

- Name
- Email
- Telephone number
- Social security number
- Positions
- Addresses
- Other information entered in free text fields or provided as an attachment

### Categories of data subjects

A whistleblower should be able to report serious misconduct and feel confident that reports are received and handled correctly. A whistleblower can be one of the following categories:

- Employee
- Volunteer
- Trainees
- Persons who otherwise perform work under the control and direction of an operator
- Self employed persons who are members of the administrative, management or supervisory body, where the operator is a business
- Shareholders operating in the company, if the operator is a limited liability company
- The processing also includes employees of the data controller who are registered as administrators in the system.

### Logs

The vendor should log agent activity in the system.

### Transfer of personal data to third countries

Personal data may not be transferred to third countries, i.e. countries outside the EU.

### Time to deleting of data

Personal data is deleted as soon as the assignment is completed or when the data is no longer needed to complete the Personal Data Processor's assignment, unless the data is to be retained according to law or other statute.

Deletion is done after the personal data controller has completed a case and marked it as handled.

## **Practical handling**

Appointed persons at the personal data controller get access to the processing tool through personal login and can manage and share necessary information linked to a case directly in the system tool.

## **Data protection by design**

The Personal Data Processor has taken the following technical and organizational measures for data protection by design and data protection by default:

- Named user accounts for the data controller
- Secure processing of login credentials and personal user accounts
- Features for built-in data protection in accordance with GDPR, such as register extracts
- Continuous erasure of personal data and logging of personal data processing
- Erasure of personal data at the conclusion of a contract

## **Sub-processors**

The supplier works with subcontractors for data storage and case reception by telephone according to information on [lantero.se](https://lantero.se).

Subcontractors for investigative work are proposed and confirmed in connection with the processing of specific cases directly in the system.