



## **Agreement on the Processing of Personal Data**

**Updated: 17 November 2022**

This agreement concerning the processing of personal data (hereinafter referred to as the “**Data Processing Agreement**”) is an integral part of the Agreement between Keskuskauppakamarin Palvelu Oy (hereinafter referred to as the “**Finland Chamber of Commerce**” or the “**Processor**”) and the organisation using the Notification Channel service (hereinafter referred to as the “**Customer**” or “**Controller**”). In this Data Processing Agreement, the Finland Chamber of Commerce and the Customer may be referred to jointly as the “**Parties**” and separately as the “**Party**”.

The following Appendices form an integral part of this Data Processing Agreement:

Appendix 1: The Finland Chamber of Commerce’s Information Security Description

Appendix 2: Customer-approved subcontractors

In the event of any conflict between the terms of the aforementioned documents, this Data Processing Agreement and, subsequently, the Appendices, in their numerical order, take precedence.

### **1. Definitions**

The terms “**personal data**”, “**controller**”, “**processor**”, “**processing**” and “**data subject**” used in this Data Processing Agreement have the same meaning as in the EU General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as the “**General Data Protection Regulation**”).

“**Data protection regulations**” in this Data Processing Agreement mean all applicable provisions concerning the protection of personal data, including the laws implementing Directive 2002/58/EC (and any amendments thereto) and the General Data Protection Regulation.

“**Personal data breach**” means a breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data processed under this Data Processing Agreement.

### **2. Scope of the Agreement**

This Data Processing Agreement applies when the Finland Chamber of Commerce processes personal data on behalf of the Customer for the purpose of providing the Service on the basis of the Agreement concluded by the Parties.

When processing personal data, the Finland Chamber of Commerce is the processor of personal data and the Customer is the controller.

This Data Processing Agreement defines the contractual terms concerning the processing of personal data and data protection, which are binding on the Customer and the Finland Chamber of Commerce, according to which the Finland Chamber of Commerce processes personal data on behalf of the Customer.



### **3. Description of the processing of personal data**

#### **3.1. Nature and purpose of the processing of personal data**

The purpose of the Finland Chamber of Commerce's processing of personal data is to enable the technical maintenance of the Service.

#### **3.2. Scope of the processing, types of personal data and categories of data subjects**

The Finland Chamber of Commerce processes the personal data of the Customer's main users. The processed personal data includes contact information (name, email address, telephone number) as well as technical identifiers and logs (IP addresses, login log, change log).

In addition, the Finland Chamber of Commerce processes notifications submitted through the Service which may include personal data depending on the nature of the notification in accordance with the General Data Protection Regulation. In the Service, notifications can be submitted by Notifiers, including Customer's current and former employees, jobseekers, the Customer's shareholders, the employees of the Customer's subcontractors, suppliers, the Customer's potential voluntary workers, trainees and other stakeholders. For the sake of clarity, it is stated that the Finland Chamber of Commerce does not read or otherwise process the content of the notifications submitted through the Service, but the processing of the notifications by the Finland Chamber of Commerce is limited to the technical processing in order to provide and maintain the Service.

### **4. Principles, responsibilities and instructions for the processing of personal data**

#### **4.1. Written instructions from the Customer**

The written instructions on the processing of personal data given to the Finland Chamber of Commerce by the Customer are provided in this Data Processing Agreement and in the Agreement. During the period of validity of this Data Processing Agreement, the Customer has the right to give new written instructions to the Finland Chamber of Commerce or to change the written instructions given to the Finland Chamber of Commerce. The provision of the Customer's new written instructions to the Finland Chamber of Commerce requires a written agreement between the Parties. The Finland Chamber of Commerce has the right to charge reasonable additional costs of complying with the amended or new written instructions issued by the Customer.

#### **4.2. The Customer's responsibility for the lawfulness of the processing**

The Customer undertakes to process personal data in accordance with the Data protection regulations. The Customer is also responsible for ensuring that all data subjects whose personal data is processed in the Service have received the notifications and information required by the Data protection regulations in relation to the processing of personal data. The Customer is responsible for ensuring that the processing of personal data and the purpose and bases of such processing are compliant with the Data protection regulations. In addition, the Customer is responsible for ensuring that personal data has been collected in accordance with the Data protection regulations and that the Customer has the right to transfer personal



data to the Finland Chamber of Commerce for processing in accordance with this Data Processing Agreement.

#### **4.3. Transfer of data outside the EU or EEA**

Personal data is not transferred outside the EU or EEA.

#### **4.4. Obligation of the Finland Chamber of Commerce to comply with the instructions given by the Customer**

The Finland Chamber of Commerce undertakes to process personal data in accordance with the Data protection regulations, the Customer's instructions described in section 4.1 and this Data Processing Agreement.

The Finland Chamber of Commerce notifies the Customer if the instructions given by the Customer are incomplete or if the Finland Chamber of Commerce suspects that they are unlawful, unless the applicable legislation prevents such communication.

### **5. Subcontractors**

The Finland Chamber of Commerce has the right to use subcontractors, which the Customer has approved, in the processing of personal data. At the time of the entry into force of this Data Processing Agreement, the Customer has given its consent to the use of the subcontractors listed in Appendix 2.

The Finland Chamber of Commerce must notify the Customer of the addition of a new subcontractor processing personal data in accordance with this Data Processing Agreement at least thirty (30) days before the start of the processing of personal data by the subcontractor in question. The Customer may prohibit the use of a new subcontractor only if the Customer has a reasonable doubt about the ability of the new subcontractor to comply with the Data protection regulations. If the Customer does not prohibit the use of the new subcontractor in writing within fourteen (14) days of the Finland Chamber of Commerce's notification, the Finland Chamber of Commerce may use the new subcontractor in the processing of personal data.

The Finland Chamber of Commerce ensures by appropriate means that subcontractors comply with the obligations equivalent to this Data Processing Agreement. The Finland Chamber of Commerce is responsible for the activities of its subcontractors as if they were its own.

### **6. Protection of personal data**

#### **6.1. The Finland Chamber of Commerce's responsibility**

The Finland Chamber of Commerce takes appropriate technical and organisational measures to prevent and combat unauthorised and unlawful processing of personal data and to prevent any accidental or unlawful loss, alteration, destruction, damage, disclosure of, or access to personal data.

#### **6.2. The Customer's responsibility**

The Customer ensures the appropriate and sufficient information security of the equipment and IT operating environments for which the Customer is responsible.



Unless agreed otherwise, the Customer is responsible for backing up personal data and for checking the functioning of the backups. The Customer is responsible for informing the Finland Chamber of Commerce of any matters related to personal data provided by the Customer, such as risk assessments and the processing of special categories of personal data, which have an effect on the technical and organisational measures that are implemented in accordance with this Data Processing Agreement.

### **6.3. Information security of the Service**

The Finland Chamber of Commerce's Information Security Description (Appendix 1) which describes the principles and methods of personal data protection in more detail is an integral part of this Data Processing Agreement.

## **7. The Finland Chamber of Commerce's duty to assist**

Considering the nature of the processing operations and the information available to the Finland Chamber of Commerce, the Finland Chamber of Commerce undertakes to:

- i. assist the Customer with appropriate technical and organisational measures to fulfil the Customer's obligation to respond to the data subject's request for information concerning the rights of the data subjects in accordance with the Data protection regulations;
- ii. assist the Customer in fulfilling its obligations under the Data protection regulations in relation to information security, Personal data breaches, data protection impact assessment and prior consultation; and
- iii. make available to the Customer all such information necessary to demonstrate compliance with this Data Processing Agreement and the Data protection regulations.

The Finland Chamber of Commerce has the right to charge the Customer for the additional costs reasonably incurred in complying with this section 7.

## **8. Personal data breaches**

The Processor must notify the Controller of any Personal data breach coming to its attention without undue delay. In connection with the notification of a Personal data breach, the Customer must provide the Supplier with all the information that can be considered to help in the investigation, limitation or prevention of the Personal data breach.

The following information must be included in the Supplier's Personal data breach notification to the Customer:

- a) a description of the Personal data breach, including, where possible, the categories and estimated numbers of data subjects concerned and the categories and estimated numbers of personal data types (to the extent that such data are available to the Finland Chamber of Commerce);
- b) The contact information of the Data Protection Officer of the Finland Chamber of Commerce or any other person from whom further information may be obtained;
- c) a description of the likely consequences of the Personal data breach; and



- d) a description of the measures taken by the Finland Chamber of Commerce due to the Personal data breach and any measures taken by the Finland Chamber of Commerce to mitigate the adverse effects of the Personal data breach.

If it is not possible to provide the above information at the same time, the information may be delivered section by section.

The Finland Chamber of Commerce must document the Personal data breaches and hand over the documentation to the Customer, upon its request.

After becoming aware of a Personal data breach, the Finland Chamber of Commerce must ensure the safeguarding of personal data and, in cooperation with the Customer, take appropriate measures to ensure the protection of personal data.

The Customer is responsible for the necessary notifications to the data protection authorities.

## **9. Auditing**

An independent auditor authorised by the Customer has the right to audit the Finland Chamber of Commerce's compliance with the obligations under this Data Processing Agreement. The Finland Chamber of Commerce must allow the audits authorised by the Customer and participate in them in a reasonable manner.

The Customer is responsible for all the costs caused by the audit and must reimburse the Finland Chamber of Commerce for the costs caused by the audits. If the audits reveal significant deficiencies in the activities of the Finland Chamber of Commerce, the Finland Chamber of Commerce is responsible for its own costs arising from the audits.

The audit may be carried out no more than once a year and the Finland Chamber of Commerce must be notified of it in writing at least thirty (30) days in advance. The audit must be carried out in a way that does not interfere with the commitments of the Finland Chamber of Commerce and its subcontractors to third parties.

The auditor must sign the normal non-disclosure agreements.

The auditor cannot be a competitor of the Finland Chamber of Commerce and the audit cannot be carried out after the termination of this Data Processing Agreement.

## **10. Erasing or returning personal data to the Controller at the end of the processing**

Upon termination of the Data Processing Agreement, the Finland Chamber of Commerce must, on the basis of the Customer's decision, either erase or return all personal data processed on behalf of the Customer to the Customer or a third party designated by the Customer and destroy any copies of the personal data, unless the Data protection regulations or an authority's order requires the retention of personal data. If the Customer requests that the personal data be returned to the Customer or transferred to a third party, the Customer is obliged to compensate the Finland Chamber of Commerce for the reasonable costs of returning or transferring the personal data.



### **11. Limitation of liability**

This Data Processing Agreement is subject to the terms of the Agreement regarding limitation of liability.

### **12. Validity**

This Data Processing Agreement will take effect when the Customer has deployed the Service. The terms of the Data Processing Agreement are valid for as long as the Customer uses the Service, except for terms that are intended to remain in force even after the termination of the use of the Service.

### **13. Contact information of the Finland Chamber of Commerce**

Keskuskauppakamarin Palvelu Oy  
[tietosuoja@kauppakamari.fi](mailto:tietosuoja@kauppakamari.fi)



## **Appendix 1: The Finland Chamber of Commerce's Information Security Description**

The Finland Chamber of Commerce is committed to the appropriate information security practices. The information contained in the register processed electronically is protected by firewalls, passwords and providing two-stage authentication as well as by other generally accepted technical means in the field of information security. The data transfer between the Customer and the Finland Chamber of Commerce is encrypted by the SSL (Secure Socket Layer) technology or another solution commonly classified as data secure.

The Finland Chamber of Commerce protects the Customer's data from unauthorised use and distribution. Only the designated representatives of the Finland Chamber of Commerce have access to the information contained in the register on the basis of separately granted access rights. All notifications and attachments submitted to the Service are encrypted at the time of submitting. The decryption and plain language reading of the notifications are only possible with the IDs of the processors pre-authorised by the Customer. The Finland Chamber of Commerce cannot decrypt an encryption even at the request of the Customer. Users' access rights are controlled, and the creation of unsafe combinations of access rights is prohibited by the access right management policy and their creation is controlled as part of the access right management.

Access rights are reviewed regularly and removed when the user no longer needs them. The Customer is responsible for notifying the Finland Chamber of Commerce of the expired access rights. The access rights of representatives who have left the Finland Chamber of Commerce must be immediately removed from all systems at the end of their employment. The Customer's data is processed only by the representative of the Finland Chamber of Commerce who is assigned for the work in question. Processing of personal data on other grounds is prohibited even if the representative of the Finland Chamber of Commerce has technical access to the customer data on the basis of their work task and business reasons.

All employees of the Finland Chamber of Commerce and third parties working on its behalf are bound by the obligation of confidentiality with regard to all customer information and personal data. The obligation of confidentiality is recorded in the employment contracts of the Finland Chamber of Commerce employees, including sanctions. The obligation of confidentiality is recorded in agreements with third parties, including sanctions.

The Finland Chamber of Commerce uses versatile access management and change data log methods whenever possible.

Employees processing the Customer's data are trained through regular training sessions, where the legitimacy of the work is an integral part of the training. The information security and data protection awareness of the employees of the Finland Chamber of Commerce is regularly maintained in different ways: by organising regular information security and data protection briefings for all the company's employees and by organising mandatory annual training for employees in the field of information security and data protection, after which the employee must successfully pass the relevant test in order to complete the training.

The Finland Chamber of Commerce has an information security policy, which every new employee goes through when starting work at the Finland Chamber of Commerce. The existence and location of an information security policy is



communicated through regular information security training sessions, and the employees are reminded of the binding nature of the policy. The information security policy describes the general information security and data protection rules that are binding on the employee – technical rules, information security processes or policies and guidelines that are suitable for everyday work. The Customer's data is processed in information systems located in the data centre in Finland or in cloud services located in the European Union. These data centres use security practices, access management and monitoring certified by the service provider. Manually maintained materials are located in premises that have been blocked from unauthorised access by access control, and video surveillance is used in the main premises to identify and verify a potential physical security breach.

The Finland Chamber of Commerce carries out internal and third-party audits covering the technical security of critical information systems as well as the processes and guidelines concerning administrative information security and data protection.



**Appendix 2: Customer-approved subcontractors**

The Customer has approved the use of the following subcontractors:

| Subcontractor  | Purpose of the processing of personal data                                 |
|--|--|
| Haltu Oy<br>2324740-1<br>Verstaankatu 1,<br>33100 Tampere,<br>Finland              | Technical development and maintenance of the Notification Channel platform |
| UpCloud Oy<br>2431560-5<br>Aleksanterinkatu 15<br>B,<br>00100 HELSINKI,<br>FINLAND | Server and network infrastructure services                                 |