

## PRIVACY POLICY

### 1. JOINT CONTROLLERS

- a) Staria Oyj, Business ID 0696081-1, address: Mikonkatu 7, 00100 Helsinki, Finland ("**Staria**");
- b) Visionbay Solutions Oy, Business ID 2632222-7, address: Mikonkatu 7, 00100 Helsinki, Finland (<https://www.naviloq.io/>, <https://naviloqapp.com/>);
- c) Staria ONE OÜ, Business ID 12956086, address: Viru Väljak 2, 10111 Tallinn, Estonia;
- d) Staria Sweden AB, Business ID 556881-5913, address: Vasagatan 28, 111 20 Stockholm, Sweden;
- e) Staria Norway A/S, Business ID 925 088 285, address: Grenseveien 21, 4313 Sandnes, Norway;
- f) Staria Czechia S.R.O., Business ID 09661956, address: Jugoslavská 620/29 2, Prague 10200, Czech Republic;
- g) SuiteSpot AB, Business ID 556781-7001, address: Riddargatan 7 A, 114 35 Stockholm, Sweden; and
- h) Staria Limited, Business ID 14972808, address: First Floor, 5 Fleet Place, London, United Kingdom, EC4M 7RD.

The above entities (a) – (h) are hereinafter referred collectively as the "**Joint Controllers**" and each separately as a "**Joint Controller**".

### 2. PURPOSE OF POLICY

- 2.1 This privacy policy explains how Joint Controllers process the personal data of representatives of customers and prospects, as well as the personal data of persons visiting the Joint Controllers' websites and social media channels, and of the persons sending messages via forms or other means. In this policy, each such person is defined as a "person" or a "data subject".
- 2.2 The Joint Controllers are companies within Staria group and share a customer relationship management platform and a customer and prospect database. This privacy policy thus also defines the roles and responsibilities related to the personal data processing as Joint Controllers.
- 2.3 Provision of personal data to Joint Controllers is voluntary. If the Joint controllers do not have the personal data they need, Joint Controllers might not however be able to cooperate with the customer or prospect as intended or to respond to the person's questions.
- 2.4 A Joint Controller and its customer may also have entered into a data processing agreement regarding the processing of the customer's personal data in the provision of the Joint Controller's services, in which case the Joint Controller acts as the processor and the customer as the controller of the personal data. In such cases, the terms of the data processing agreement take precedence over this privacy policy, and the person shall contact the person's employer or other organization regarding the person's personal data.

### 3. CONTACT INFORMATION AND DATA PROTECTION OFFICER

Staria Oyj  
dpo@staria.com  
Data Protection Officer: Verna Pönttämä

Staria Oyj is the person's central contact point. You can contact the Joint Controllers via the email mentioned above. You may also contact other Joint Controllers directly. Staria and other Joint Controllers will coordinate in order to respond to your inquiry, and Staria or another Joint Controller may respond to your inquiry.

### 4. PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

- 4.1 "Personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- 4.2 All of the following information might not actually be personal data. For example, if the information only identifies a company, such as a Joint Controllers' customer company, the information is not personal data.
- 4.3 The register contains the following information:
- a) name;
  - b) person's role in organization;
  - c) address, phone number and/or email address;
  - d) possibly other contact information;
  - e) employer or other organization;
  - f) information required under laws on preventing money laundering and terrorist financing;
  - g) language;
  - h) information necessary for billing purposes;
  - i) interests (as defined by the person, and marketing preferences, and the person's reactions to advertising and marketing)
  - j) questions and contact requests addressed to Joint Controllers;
  - k) information on whether a person has opened an email message and/or clicked on a link in the message;
  - l) information on browsing on the site; and
  - m) information collected by cookies potentially containing personal data.

### 5. PURPOSES OF PROCESSING AND LEGAL BASIS FOR PROCESSING

- 5.1 Personal data is used for the following purposes:
- a) Offering Joint Controllers' products and services, fulfilling contractual obligations or in order to take steps prior to entering into a contract, and exercising Joint Controllers' contractual rights. "The legitimate interests pursued by Joint Controllers" is the legal basis for the processing of personal

data for this purpose.

- b) Creating statistics and analyses on the use of the Joint Controllers' website(s), social media channels, products and services, as well as the development of the Joint Controllers' products, services and business. "The legitimate interests pursued by Joint Controllers" is the legal basis for the processing of personal data for this purpose. Once this personal data is anonymized, it no longer constitutes personal data.
- c) Taking care of data security. "Legal obligations" is the legal basis for the processing of personal data for this purpose.
- d) Preventing fraud. "The legitimate interests pursued by Joint Controllers" is the legal basis for the processing of personal data for this purpose.
- e) For managing the customer relationship as well as for administration and management of possible reclamations. "The legitimate interests pursued by Joint Controllers" is the legal basis for the processing of personal data for this purpose.
- f) Marketing and direct marketing of the Joint Controllers' products and services, as well as providing information on the Joint Controllers' products and services, delivering newsletters, invitations and bulletins, producing and targeting targeted advertising, communications and content, optimizing marketing activities, and organizing events. When consent is required for these actions according to the legislation, "consent" is the legal basis for the processing personal data for this purpose. If the legislation does not require consent for these actions, "the legitimate interests pursued by Joint Controllers" is the legal basis for the processing of personal data for this purpose.

## 5.2 The legal basis for the processing of personal data:

- a) To the extent stated in section 5.1, the legal basis for the processing is the consent given by the person for the processing of personal data. When processing is based on the person's consent, the person has the right to withdraw the consent. However, the withdrawal of consent does not affect the lawfulness of processing carried out before such withdrawal.
- b) To the extent stated in section 5.1, the legal basis for processing is the compliance with Joint Controllers' legal obligation.
- c) To the extent stated in section 5.1, the legal basis for processing is the "legitimate interests pursued by Joint Controllers". The Joint Controllers have conducted a balance test regarding its legitimate interests. The legitimate interests may include, for example, a customer relationship or other processing that the person can reasonably expect, and the interests or fundamental rights and freedoms of the person requiring protection of personal data do not override such legitimate interests. It is typical that businesses and organizations market their services and products to other businesses and organizations. The interests and fundamental rights and freedoms of persons are respected, specific categories of personal data are not processed, and persons can reasonably expect such processing.

## 6. SOURCES OF PERSONAL DATA

- a) From the person.
- b) From the person's organization.
- c) From marketing data sources.
- d) From third parties mentioned in section 7.
- e) Personal data possibly collected by cookies.

## 7. RECIPIENTS OF PERSONAL DATA

Regular recipients of personal data are:

- a) ICT service providers or other service providers who process personal data to provide services to the Joint Controllers. Further information on the service providers is available in Appendix 1.
- b) Other service providers/data controllers. Further information on them is available in Appendix 1.
- c) Personal data possibly collected by cookies according to the cookie-related information on the Joint Controllers' website(s). Information on certain technologies is also available in Appendix 1.

## 8. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

- 8.1 The service providers used by the Joint Controllers could transfer personal data to countries outside the European Economic Area (EEA) or the European Union (EU) ("**Third Countries**").
- 8.2 The legal basis for the transfer of the personal data to Third Countries are the Binding Corporate Rules, the European Commission's Standard Contractual Clauses for the transfer of personal data to processors established in third countries ("**Standard Contractual Clauses**"), the EU-U.S. Data Privacy Framework, the European Commission's decision on adequate level of data protection of another country, alternative data export mechanisms for the lawful transfer of personal data (as recognized under EU data protection laws) or another legal basis. [The Standard Contractual Clauses are available here.](#) Further information is also available in Appendix 1.

## 9. PERIOD FOR WHICH PERSONAL DATA WILL BE STORED

- 9.1 The Joint Controllers process personal data as long as necessary to fulfill the purposes defined in this privacy policy in accordance with the applicable legislation.
- 9.2 The retention period of personal data depends on the type of the personal data and on the legal basis for the processing. For example:
  - a) Prospect information is updated, and outdated information is deleted as soon as changes are known. Prospect information is regularly reviewed and outdated information deleted at least annually. Information on organizing events (including participation in events) is stored typically for 2 years.
  - b) The personal data of representatives of current and former contractual partners is processed as long as necessary to verify and fulfill the

responsibilities and obligations between the parties and as necessary for the establishment, exercise or defence of legal claims, if the processing of the personal data is necessary for this purpose. Pursuant to Finnish legislation, there is typically a legal basis to store this personal data for 3-10 years.

- c) Information on requests from data subjects and the implementation of data subjects' rights can be stored as long needed for the purpose of fulfillment and verifying and evidencing the fulfillment of data subjects' rights. Pursuant to Finnish legislation, there might be a legal basis to store this personal data typically for 10 years.
- d) Pursuant to Finnish Accounting legislation, Staria and other Finnish Joint Controllers must retain accounting material for a period of 6 to 10 years, depending on the type of material.
- e) Pursuant to Finnish legislation on Preventing Money Laundering and Terrorist Financing, data concerning customer due diligence and customer transactions are retained for a period of 5 years after the end of the permanent customer relationship.
- f) Cookie collected information is stored as set out in the cookie-related notice on the on the Joint Controllers' website(s).
- g) Unless already anonymized when statistics and analyses have been created or when used in development, personal data collected for these purposes is deleted typically annually.
- h) If there is a suspicion of fraud or data security breach, the personal data is retained as long as necessary to investigate the suspected fraud or data security breach as well as long as is necessary for the establishment, exercise or defence of legal claims. Depending on the individual case, in these cases the personal data may be typically stored for 2—10 years or until the completion of an initiated official process, whichever is earlier.

- 9.3 The personal data is processed for longer than the above-mentioned time periods, if the personal data in question is necessary for the establishment, exercise or defence of legal claims.

## 10. PRINCIPLES OF DATA SECURITY

Staria is responsible for implementing appropriate technical and organizational measures to protect the processing of personal data. Staria uses its own and its service providers' tools, such as firewalls, encryption technologies, passwords and antivirus software, in order to prevent unauthorized access to personal data. The other Joint Controllers comply with all such measures and support, as required, in the implementation.

## 11. RIGHT OF ACCESS

- 11.1 The person has the right to obtain confirmation from Staria or another Joint Controller as to whether or not personal data concerning him or her is being processed by a Joint Controller.
- 11.2 Where such personal data is being processed by a Joint Controller, Staria or the other Joint Controller shall provide the person with a copy of the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of personal data, in particular recipients in third countries or international organizations;
- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the existence of the right to request from a Joint Controller rectification or erasure of personal data or restriction of processing of personal data concerning the person or to object to such processing;
- f) the right to lodge a complaint with a supervisory authority;
- g) available information on the source the personal data;
- h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the person;
- i) where personal data is transferred to a Third Country or to an international organization, information on the appropriate safeguards.

11.3 For any further copies requested by the person, Joint Controllers may charge a reasonable fee based on administrative costs.

## 12. RIGHT TO RECTIFICATION

The person shall have the right to obtain from Staria or another Joint Controller without undue delay the rectification of inaccurate personal data concerning the person. Taking into account the purposes of the processing, the person shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. Staria is mainly responsible for and carrying out the rectification of inaccurate personal data and the erasing of personal data when necessary, and other Joint Controllers provide information and assist Staria when necessary.

## 13. RIGHT TO ERASURE

13.1 The Joint Controller or Staria erases the personal data concerning the person upon the person's request where one of the following grounds applies:

- a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- b) the person withdraws the consent on which the processing is based;
- c) the person objects to the processing pursuant to section 15 and there are no overriding legitimate grounds for the processing;
- d) the personal data has been unlawfully processed;
- e) the personal data has to be erased for compliance with a legal obligation in applicable law to which the Joint Controller is subject;

- f) the personal data has been collected in relation to the offer of information society service.

13.2 However, the Joint Controller or Staria does not have an obligation to erase personal data to the extent the processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) to comply with a legal obligation requiring the processing;
- c) for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes; or
- d) for the establishment, exercise or defence of legal claims.

## 14. RIGHT TO RESTRICTION OF PROCESSING

14.1 **"Restriction of processing"** means the marking of stored personal data with the aim of limiting its processing.

14.2 The person has the right to obtain from a Joint Controller restriction of processing where one of the following applies:

- a) the accuracy of the personal data is contested by the person, for a period enabling the Joint Controllers to verify the accuracy of the personal data;
- b) the processing is unlawful and the person opposes the erasure of the personal data and requests the restriction of its use instead;
- c) the Joint Controllers no longer need the personal data for the purposes of the processing, but the personal data is required by the person for the establishment, exercise or defence of legal claims;
- d) the person has objected to processing pursuant to section 15 pending the verification whether the legitimate grounds of Joint Controllers override those of the person.

14.3 In the aforementioned situations, Joint Controllers process the personal data only in the following circumstances:

- a) based on the person's consent;
- b) for the establishment, exercise, or defense of legal claims;
- c) for the protection of another person's rights; or
- d) for reasons of public interest of the European Union or a Member State.

## 15. RIGHT TO OBJECT

The person has the right to object, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her where the processing is based on either of the following legal basis: (i) the processing is necessary for the performance of a task carried out in the public interest or (ii) the processing is necessary for the purposes of the legitimate interests pursued by Joint Controllers or by a third party. Joint Controllers shall no longer process the personal data unless Staria or another Joint Controller demonstrates compelling legitimate grounds for the processing which override the interests,

rights and freedoms of the person, or unless any of the Joint Controllers needs to process the personal data for the establishment, exercise or defence of legal claims.

## **16. RIGHT TO DATA PORTABILITY**

At the person's request, if a Joint Controller processes the personal data based on the person's consent or based on a contract with the person and if the processing is carried out by automated means:

- a) Staria or the Joint Controller shall provide the person with the personal data which he or she has provided to the Joint Controller, in a structured, commonly used and machine- readable format; and
- b) if technically feasible, Staria or the Joint Controller shall transmit the personal data in the same format directly to another controller.

## **17. RIGHT TO LODGE COMPLAIN WITH SUPERVISORY AUTHORITY**

If the person believes that Joint Controllers' processing of personal data infringes regulatory data protection requirements, the person may lodge a complaint with the supervisory authority. The contact details of the Finnish supervisory authority can be found here:

<https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>

## **18. AUTOMATED DECISION MAKING**

Joint Controllers are not using automated decision-making meant in the General Data Protection Regulation (GDPR).



## APPENDIX 1 PROCESSORS AND OTHER DATA CONTROLLERS

Joint Controllers utilize the following third-party services. These parties process personal data on behalf of Joint Controllers as processors, or as controllers according to their own privacy policies. Additionally, Joint Controllers use other cookie technologies, and information on the data collected by them and their usage can be obtained from the cookie-related information on Joint Controllers' website(s).

Name	Additional information
StarIT Oy Keilaranta 15, 02150 Espoo, Finland	Data Center Services and ICT Support. Personal Data in the EEA Area. Subcontractor Ficolo Oy.
Dealfront/Leadfeeder	<a href="https://marketing.dealfront.com/inside-eea-data-processing-agreement-dealfront-en.pdf">https://marketing.dealfront.com/inside-eea-data-processing-agreement-dealfront-en.pdf</a>
Lytyi	<a href="https://www.lyyti.com/en/data-protection-security">https://www.lyyti.com/en/data-protection-security</a>
Gotowebinar GoTo Group, Inc.	<a href="https://www.goto.com/-/media/pdfs/trust---resource-center/goto-customer-dpa.pdf">https://www.goto.com/-/media/pdfs/trust---resource-center/goto-customer-dpa.pdf</a>
HubSpot	<a href="https://legal.hubspot.com/dpa">https://legal.hubspot.com/dpa</a> <a href="https://legal.hubspot.com/sub-processors-page">https://legal.hubspot.com/sub-processors-page</a>
Trustmary	<a href="https://trustmary.com/data-protection-addendum/">https://trustmary.com/data-protection-addendum/</a>
Vimeo	<a href="https://vimeo.com/privacy">https://vimeo.com/privacy</a>
Youtube	<a href="https://www.youtube.com/intl/ALL_ie/howyoutubeworks/user-settings/privacy/">https://www.youtube.com/intl/ALL_ie/howyoutubeworks/user-settings/privacy/</a>
Meta	Advertising and marketing, analytics <a href="https://www.facebook.com/policy">https://www.facebook.com/policy</a>
WordPress	The use of Staria's website <a href="https://automattic.com/privacy-notice/">https://automattic.com/privacy-notice/</a> <a href="https://automattic.com/cookies/">https://automattic.com/cookies/</a> <a href="https://mailchimp.com/legal/privacy/">https://mailchimp.com/legal/privacy/</a> <a href="https://mailchimp.com/legal/cookies/">https://mailchimp.com/legal/cookies/</a>
Google Tag Manager	Tag management <a href="https://policies.google.com/technologies/partner-sites">https://policies.google.com/technologies/partner-sites</a>
Google Analytics	Advertising and marketing, analytics <a href="https://policies.google.com/technologies/partner-sites">https://policies.google.com/technologies/partner-sites</a>
Linkedin	Advertising and marketing, analytics <a href="https://www.linkedin.com/legal/privacy-policy">https://www.linkedin.com/legal/privacy-policy</a>