

Data Processor agreement

Between controller and Processor

This agreement has on the date of signature been concluded between the parties;

- 1)
with Company Registration number (controller)

and
- 2) **Seriline AB**
with Company Registration number 556389–8609 (Processor)

1 Definitions

If this agreement contains concepts that correspond to regulation 2016/679 ("GDPR") of the European Parliament and of the Council, the concepts shall be interpreted and applied according to GDPR.

2 Content and purpose

This processor agreement has been established to meet the requirements in Article 28, GDPR.

The processor will process personal data to the extent that is required to fulfil the commitments towards the controller.

3 Responsibilities and instructions

The processor is responsible for all processing of contracted personal data in accordance to GDPR.

The processor undertakes to treat personal data only in accordance with instructions given in writing by the controller. The processor may only process personal data on documented instructions from the controller.

The processor undertakes to process the personal data in accordance GDPR, as well as the Swedish Data Protection Authority, or relevant EU agency's regulations, positions and recommendations in the personal data field, hereinafter referred to as the applicable law.

The processor may not, without injunction from relevant authority or mandatory legislation:

- a) collect or disclose personal data from or to any third party unless otherwise agreed in writing.
- b) change method of processing
- c) copy or replication personal data;

or in any other way process personal data for purposes other than those in accordance with the commitments against the controller.

The processor may not, (i) without prior written authorisation of the controller, and (ii) ensuring that such transfer is in accordance with applicable law, transfer any personal data to countries outside of EEA or to countries that are not covered by the exemption for prohibition on transfer to third countries according to applicable law. To avoid misunderstandings, this prohibition also includes technical support, maintenance and similar services.

If the processor suspects, alternatively detects any security offence as unauthorised access, destruction, alteration or similarly of personal data, or if the processor for any other reason cannot fulfil the obligations of this agreement, the processor shall immediately (i) investigate the personal data breach and take appropriate action to heal the incident and prevent a repeat, and (ii) provide the controller with a description of the personal data breach.

The notification of the personal data breach shall at least

- a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- c) describe the likely consequences of the personal data breach;
- d) describe the measures taken or proposed to be taken by the processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The processor shall inform the controller if the processor gets knowledge of that personal data has been processed in violation of the processor's instructions or this processor agreement.

Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the processor shall, to a reasonable extent, prior to the processing help the controller to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

4 Security and privacy

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the processor shall, to reasonable extent, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- a) the pseudonymisation and encryption of personal data
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The processor shall ensure that the access control is correct and that confidentiality is complied.

The processor shall ensure that all employees, consultants and other persons for whom the processor is responsible and who process personal data are bound by an appropriate confidentiality obligation and are informed of how processing of personal data may be processed. The processor is responsible for the persons who have access to the personal data are informed of how they may process the personal data in accordance with instructions from the controller.

5 Audit and visits

The controller is entitled to carry out an audit against the processor, conducted by the controller or another auditor mandated by the controller, or in other way check that the processor's processing of personal data complies with this agreement. In case of such audit or control, the assistant shall provide the controller the assistance required for the audit.

The processor shall on action taken on a request provide all available information regarding the processing of personal data in order for the controller to fulfil his obligations as controller under applicable law.

For those cases data subjects, Swedish Data Protection Authority or other third parties requesting information from the controller or processor regarding the processing of personal data, the parties shall cooperate and exchange information to the extent it is required. No party may disclose personal data without prior consent from the counterparty except in cases where there is an injunction from the relevant authority or if a party is required under mandatory legislation.

The processor shall assist the controller in the appropriate manner through appropriate technical and organisational measures, so that the controller can fulfil his duty regarding the rights of the data subjects in accordance with Chapter III of the GDPR.

6 Sub-processors

The controller is aware and accepts that the processor will hire subcontractors to fulfil their obligations (below “sub-processors”), and that therefore, personal data on behalf of the controller will also be processed by these sub-processors.

In so far the processor hires sub-processor, these shall be approved by the controller unless otherwise has been agreed in writing between the parties.

If the processor hires a sub-processor, the processor has mandate and obligation to conclude special agreements with such sub-processor regarding the sub-processor’s processing of personal data. Such agreement shall stipulate that the sub-processor has the corresponding obligations that the processor has under this agreement.

The processor shall, at the request of the controller, provide the parts of the processor’s agreement with the sub-processor required to prove that the processor has fulfilled his obligations under this agreement.

The processor shall keep a correct and up-to-date list of the sub-processor used for processing personal data and where these are geographically located. At the request of the controller, the processor shall, without delay, provide contact details to the sub-processor handling personal data.

The processor shall inform the controller of any plans to hire new sub-processors or substitute sub-processors.

7 Liability

The processor shall hold the controller harmless in the event of liability arising from damage attributable to the processor's processing of personal data contrary to written instructions from the controller. The responsibility does not include indirectly damage and is limited to the amount paid by the controller for the processor services and products in the last 12 months prior to the incident.

8 Cessation of processing of personal data

The processor shall, depending on what the controller selects, delete or return all data containing personal data to all media on which it is fixed after the assignment has been completed and delete existing copies.

9 Dispute

Disputes arising from this agreement shall be settled by arbitration in accordance with the Rules for Expedited Arbitrations of Stockholm Chamber of Commerce.

This Agreement has been executed in two duplicate copies, each party has received one.

Controller

Place and date

Company name

Signature

Name in block letters

Processor

Bromma

Place and date

Seriline AB

Company name

Signature

Freddie Parrman, CEO

Name in block letters

**Return address for Data Processor
agreement**

Company name

Address row 1

Address row 2

Zip & city

Return **two** signed copies of the
agreement to:

Seriline AB
Att: GDPR
Gustavslundsvägen 50
167 51 Bromma
Sweden