
DATA PROCESSING AGREEMENT

Agreement pursuant to Article 28.4 of Regulation (EU) 2016/679 (General Data Protection Regulation).¹

Contents

1. Parties, roles, contact details and contact persons	2
2 Definitions	3
3 Background and Purpose	4
4 Processing of Personal Data and Specification	4
5 The Controller's Undertakings	4
6 The Processor's Undertakings	4
7 Security Measures	5
8 Confidentiality	5
9 Audit, Supervision and Inspection	6
10 Data Subject Rights	6
11 Personal Data Breaches	7
12 Sub-processors	7
13 Transfer of Personal Data to a Third Country	8
14 Liability for Damage in Connection with Processing	8
15 Execution, Term and Termination of the DPA	8
16 Amendments and Termination with Immediate Effect, etc.	9
17 Measures upon Termination of the DPA	9
18 Notices under this DPA and Instructions	9
19 Contact Persons	10
20 Responsibility for Party Information and Contact Details	10
21 Dispute Resolution	10
22 Execution of the DPA	10
Appendix 1 Controller's Instructions for the Processing of Personal Data	11
Appendix 2 List of Approved Sub-processors	13
Appendix 3 – Description of transfer to third countries	15

¹ Regulation (EU) 2016/679 (the General Data Protection Regulation) requires that the processing of Personal Data by a processor on behalf of the controller be governed by a written agreement.

[Gulmarkerad text inom hakparenteser tas bort innan Personuppgiftsbiträdesavtalet upprättas.]

1. Parties, roles, contact details and contact persons

Controller	Processor
Swedavia AB	[Full legal name of the organization]
Corporate registration number	Corporate registration number
556797-0818	[Specify registration number]
Registered address	Registered address
190 45 STOCKHOLM-ARLANDA	[Specify address]
Contact person for administration of this Data Processing Agreement	Contact person for administration of this Data Processing Agreement
Name: [First name and surname] Email: [Email address] Telephone: [Telephone number]	Name: [First name and surname] Email: [Email address] Telephone: [Telephone number]
Contact person for cooperation on data protection matters	Contact person for cooperation on data protection matters
Name: Data Protection Officer Email: personuppgifter@swedavia.se Telephone: +46 10-109 00 00	Name: [First name and surname] Email: [Email address] Telephone: [Telephone number]



2 Definitions

2.1 In addition to the terms defined in the main body of this Data Processing Agreement ("DPA"), the following definitions, whether used in the singular or plural, definite or indefinite form, shall have the meanings set out below when capitalized. Terms not expressly defined in this DPA shall, to the extent possible, be interpreted in accordance with or in light of the General Data Protection Regulation.

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, organization, 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

All privacy and data protection laws and regulations, as well as any other applicable laws, regulations, and binding rules applicable to the Processing carried out under this DPA, including national legislation and European Union 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 documented instructions specifying the subject matter, duration, nature and purpose of the Processing, the type of Personal Data, the categories of Data Subjects and any specific requirements applicable to the Processing.

Log

The result of Logging.

Logging

The continuous collection of information relating to the Processing of Personal Data carried out under this DPA and which can be linked to an identified or identifiable 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; 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.

Personal Data Breach

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

Data Subject

A natural person whose Personal Data is Processed.

Third Country

A country that is not a Member State of the European Union (EU) and not part of the European Economic Area (EEA).

Sub-processor

A natural or legal person, public authority, agency, or other body engaged by the Processor as a subcontractor to Process Personal Data on behalf of the Controller.

3 Background and Purpose

3.1 This Data Processing Agreement, together with the Instructions and any list of Sub-processors (collectively, the “DPA”), governs the Processor’s Processing of Personal Data on behalf of the Controller. The purpose of the DPA is to safeguard the fundamental rights and freedoms of the Data Subject in connection with the Processing, in accordance with Article 28(3) of Regulation (EU) 2016/679 (the “General Data Protection Regulation” or “GDPR”).

3.2 Where the DPA forms part of, or is incorporated into, another agreement between the Parties, that agreement shall be referred to in the DPA as the “Main Agreement”.

3.3 In the event that any matter governed by Sections 15 or 16, Sections 18–20, or Section 22 of the DPA is regulated differently in the Main Agreement, the provisions of the Main Agreement shall prevail.

3.4 References in the DPA to national or European Union legislation shall be construed as references to the legislation in force from time to 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 the provisions of this DPA.

4.2 The Controller shall provide documented Instructions to the Processor regarding how the Processing is to be carried out.

4.3 The Processor shall process Personal Data only in accordance with this DPA and the Instructions in force from time to time.

5 The Controller’s Undertakings

5.1 The Controller shall ensure that there is, at all times, a valid legal basis for the Processing and shall issue accurate Instructions, taking into account the nature of the Processing, so that the Processor and any Sub-processors are able to fulfil their respective obligations under this DPA and, where applicable, the Main Agreement.

5.2 The Controller shall, without undue delay, inform the Processor of any changes to the Processing that affect the Processor’s obligations under Data Protection Legislation.

5.3 The Controller is responsible for providing information to Data Subjects regarding the Processing and for safeguarding the rights of Data Subjects under Data Protection Legislation, as well as for fulfilling any other obligations incumbent upon the Controller pursuant to Data Protection Legislation.

6 The Processor’s Undertakings

6.1 The Processor undertakes to carry out the Processing solely in accordance with this DPA and for the specific purposes set out in the Instructions, and to comply with Data Protection Legislation. The Processor further undertakes to remain continuously informed of applicable law in this area.

6.2 The Processor shall implement appropriate measures to protect the Personal Data against any Processing that is not in accordance with this DPA, the Instructions or Data Protection Legislation.

6.3 The Processor undertakes to ensure that all natural persons acting under its authority comply with this DPA and the Instructions, and that such persons are informed of relevant data protection legislation.

6.4 Upon request from the Controller, the Processor shall assist the Controller in ensuring compliance with the obligations set out in Articles 32–36 of the General Data Protection Regulation and shall, where requested by the Controller, assist in responding to requests for the exercise of Data Subject rights in accordance with Chapter III of the GDPR, taking into account the nature of the Processing and the information available to the Processor.

6.5 Where the Processor considers that any Instruction is unclear, contrary to Data Protection Legislation, or absent, and the Processor deems that new or supplementary Instructions are required in order to fulfil its obligations, the Processor shall without undue delay inform the Controller, temporarily suspend the Processing and await further Instructions, unless the Parties agree otherwise.

6.6 Where the Controller provides new or amended Instructions, the Processor shall, without undue delay upon receipt, inform the Controller whether implementation of such Instructions will result in additional costs for the Processor. In such case, the Processor shall be entitled to compensation for reasonable additional costs subject to the Controller's approval, provided that the new or amended Instructions are not required due to a change in applicable law.

7 Security Measures

7.1 The Processor shall implement all appropriate technical and organizational security measures required under Data Protection Legislation and the Controller's Instructions in order to prevent Personal Data Breaches, by ensuring that the Processing meets the requirements of the GDPR and that the rights of the Data Subject are protected.

7.2 The Processor shall continuously ensure that the technical and organizational security measures relating to the Processing provide an appropriate level of confidentiality, integrity, availability and resilience.

7.3 Any additional or amended security requirements imposed by the Controller after the Parties have entered into this DPA shall be deemed to constitute new Instructions under the DPA.

7.4 The Processor shall, through an appropriate access control system, grant access to Personal Data only to those natural persons acting under the Processor's authority who require such access in order to perform their duties.

7.5 The Processor shall Log access to Personal Data in accordance with the Instructions. Logs shall be subject to appropriate safeguards in accordance with Data Protection Legislation.

7.6 The Processor shall regularly test, assess and evaluate the effectiveness of the technical and organizational measures implemented to ensure the security of the Processing.

8 Confidentiality

8.1 The Processor and all natural persons acting under its authority shall observe confidentiality and non-disclosure in connection with the Processing. Personal Data may not be used or disclosed for any purposes other than those agreed, whether directly or indirectly, unless otherwise agreed in writing.

8.2 The Processor shall ensure that all natural persons acting under its authority who participate in the Processing are bound by a confidentiality undertaking in respect of the Processing. This requirement shall not apply where such persons are already subject to statutory confidentiality obligations under applicable law. The Processor further undertakes to ensure that confidentiality agreements are in place with any Sub-processor and that confidentiality undertakings are entered into between the Sub-processor and all natural persons acting under its authority who participate in the Processing.

8.3 The Processor shall promptly notify the Controller of any contact with a supervisory authority relating to the Processing. The Processor shall not be entitled to represent the Controller or act on the Controller's behalf in dealings with supervisory authorities concerning the Processing.

8.4 If a Data Subject, supervisory authority or third-party requests information from the Processor relating to the Processing, the Processor shall inform the Controller thereof. The Processor shall not disclose information concerning the Processing to a Data Subject, supervisory authority or third party without the Controller's prior written consent, unless disclosure is required by mandatory law. The Processor shall assist in providing any information that is subject to such consent or legal requirement.

9 Audit, Supervision and Inspection

9.1 As part of the guarantees referred to in Article 28(1) of the GDPR, the Processor shall, without undue delay and upon request by the Controller, make available information regarding the technical and organizational measures implemented to ensure that the Processing meets the requirements of this DPA and Article 28(3)(h) of the GDPR.

9.2 The Processor shall, at least once per calendar year, review the security of the Processing by means of an internal audit to ensure compliance with this DPA. The results of such internal audit shall be made available to the Controller upon request.

9.3 The Controller shall have the right, either itself or through a third party appointed by the Controller (provided that such third party is not a competitor of the Processor), to verify that the Processor complies with the requirements of this DPA, the Instructions and Data Protection Legislation.

In connection with such audit, the Processor shall assist the Controller, or the person conducting the audit on the Controller's behalf, by providing relevant documentation and access to premises, IT systems and other assets necessary to verify the Processor's compliance with this DPA, the Instructions and Data Protection Legislation. The Controller shall ensure that personnel carrying out the audit are bound by confidentiality obligations under law or contract.

9.4 As an alternative to the procedures set out in Clauses 9.2–9.3, the Processor may offer other means of auditing the Processing, for example through an audit conducted by an independent third party. In such case, the Controller shall have the right, but not the obligation, to rely on such alternative audit mechanism. In connection with such audit, the Processor shall provide the Controller or the independent third party with the assistance necessary to carry out the audit.

9.5 The Processor shall permit a supervisory authority, or any other authority entitled to do so by law, to conduct inspections in accordance with applicable legislation in force from time to time, even if such inspection would otherwise conflict with the provisions of this DPA.

9.6 The Processor shall ensure that the Controller is granted rights vis-à-vis any Sub-processor corresponding to all rights granted to the Controller vis-à-vis the Processor under this Section 9 of the DPA.

10 Data Subject Rights

10.1 Where the Controller has requested rectification or erasure due to the Processor's incorrect Processing, the Processor shall take appropriate measures without undue delay and, in any event, no later than thirty (30) days from receipt of the necessary information from the Controller. Where the Controller has requested erasure, the Processor may process the relevant Personal Data solely as part of the rectification or erasure procedure.

10.2 If the Processor implements technical or organizational measures in the Processing (for example upgrades or troubleshooting) that may affect the Processing, the Processor shall notify the Controller in writing in accordance with the provisions on notices set out in Section 18 of this DPA. Such information shall be provided in good time prior to the implementation of the measures.

11 Personal Data Breaches

11.1 The Processor shall have the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident, in accordance with Article 32(1)(c) of the GDPR.

11.2 Taking into account the nature of the Processing and the information available to the Processor, the Processor undertakes, upon request, to assist the Controller in fulfilling its obligations in the event of a Personal Data Breach relating to the Processing. At the Controller's request, the Processor shall also assist in investigating any suspected unauthorized Processing and/or access to Personal Data.

11.3 In the event of a Personal Data Breach of which the Processor becomes aware, the Processor shall notify the Controller in writing without undue delay and, in any event, no later than forty-eight (48) hours after having become aware of the Personal Data Breach. Taking into account the nature of the Processing and the information available to the Processor, the Processor shall provide the Controller with a written description of the Personal Data Breach.

11.4 The description shall, at a minimum, include:

- a) the nature of the Personal Data Breach and, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- b) the likely consequences of the Personal Data Breach; and
- c) the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

11.5 Where it is not possible for the Processor to provide the full description at the same time as the notification referred to in Clause 11.3, the information may be provided in phases without undue further delay.

12 Sub-processors

12.1 The Processor shall be entitled to engage the Sub-processor(s) listed in the attached register of Sub-processors, Appendix 2.

12.2 The Processor undertakes to enter into a written agreement with each Sub-processor governing the Processing carried out by the Sub-processor on behalf of the Controller and to engage only Sub-processors providing sufficient guarantees. The Sub-processor shall implement appropriate technical and organizational measures to ensure that the Processing meets the requirements of Data Protection Legislation. In matters relating to data protection, the agreement shall impose on the Sub-processor obligations at least equivalent to those imposed on the Processor under this DPA.

12.3 In its agreement with the Sub-processor, the Processor shall ensure that the Controller has the right to terminate the engagement of the Sub-processor and to instruct the Sub-processor to erase or return the Personal Data if the Processor has ceased to exist in fact or in law, or has become insolvent.

12.4 The Processor shall remain fully liable to the Controller for the performance of the Sub-processor's Processing. The Processor shall promptly notify the Controller if a Sub-processor fails to fulfil its obligations under this DPA.

12.5 The Processor shall be entitled to engage new Sub-processors and replace existing Sub-processors unless otherwise specified in the Instructions.

12.6 Where the Processor intends to engage a new Sub-processor or replace an existing Sub-processor, the Processor shall ensure that the Sub-processor has the capacity and ability to fulfil its obligations under Data Protection Legislation. The Processor shall notify the Controller in writing of:

- a) the Sub-processor's name, registration number and registered office (address and country);

-
- b) the categories of Personal Data and categories of Data Subjects concerned; and
c) the location where the Personal Data will be processed.

12.7 The Controller shall have the right, within thirty (30) days from the date of notification pursuant to Clause 12.6, to object to the engagement of a new Sub-processor and, as a consequence of such objection, to terminate this DPA in accordance with Clause 16.5 of the DPA.

12.8 The Processor shall at all times maintain an accurate and up-to-date list of Sub-processors engaged to Process Personal Data on behalf of the Controller and shall make such list available to the Controller. The list shall specify, in particular, the country in which the Sub-processor processes Personal Data and the types of Processing carried out by the Sub-processor.

12.9 When the Processor ceases to use a Sub-processor, the Processor shall notify the Controller in writing. Upon termination of the agreement with a Sub-processor, the Processor shall ensure that the Sub-processor erases or returns the Personal Data.

12.10 Upon request by the Controller, the Processor shall provide a copy of the agreement governing the Sub-processor's Processing of Personal Data and the list of Sub-processors referred to in Clause 12.1.

13 Transfer of Personal Data to a Third Country

13.1 The Processor shall ensure that Personal Data is processed and stored within the EU/EEA by a natural or legal person established within the EU/EEA, unless the Parties to this DPA agree otherwise.

13.2 The Processor shall only be entitled to transfer Personal Data to a Third Country for Processing (for example for service, support, maintenance, development, operation or similar activities) where the Controller has provided its prior written approval to such transfer and issued Instructions for that purpose.

13.3 Any transfer to a Third Country for Processing pursuant to Clause 13.2 shall only take place where it complies with Data Protection Legislation and meets the requirements applicable to the Processing under this DPA and the Instructions.

14 Liability for Damage in Connection with Processing

14.1 In relation to compensation for damage arising from Processing which, pursuant to a final judgment or settlement, is payable to a Data Subject due to a breach of this DPA, the Instructions and/or applicable provisions of Data Protection Legislation, Article 82 of the GDPR shall apply.

14.2 Administrative fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Swedish Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation, shall be borne by the Party upon whom such fine has been imposed.

14.3 If either Party becomes aware of circumstances that may result in damage to the other Party in connection with the Processing, that Party shall, without undue delay, inform the other Party thereof and actively cooperate with the other Party in order to prevent and mitigate such damage.

14.4 Notwithstanding any provision of the Main Agreement to the contrary, Clauses 14.1 and 14.2 of this DPA shall prevail over any other provisions governing the allocation of liability between the Parties insofar as they relate to the Processing.

15 Execution, Term and Termination of the DPA

15.1 This DPA shall enter into force on the date it has been signed by both Parties and shall remain in effect until further notice. Either Party shall have the mutual right to terminate this DPA by giving thirty (30) days' written notice.

16 Amendments and Termination with Immediate Effect, etc.

16.1 Either Party shall have the right to terminate this DPA with immediate effect if there is a material change in the ownership structure of the other Party.

16.2 Either Party shall have the right to request a renegotiation of this DPA if applicable legislation, or the interpretation thereof, changes in a manner that materially affects the Processing. A request for renegotiation pursuant to the foregoing shall not result in the termination of any part of this DPA, but shall only entail that renegotiations are initiated.

16.3 Any amendments to or modifications of this DPA shall be made in writing and signed by both Parties.

16.4 If either Party becomes aware that the other Party is acting in breach of this DPA and/or the Instructions, it shall notify the other Party thereof without undue delay. Thereafter, the notifying Party shall have the right to suspend performance of its obligations under this DPA with immediate effect until such time as the other Party has confirmed that the non-compliant conduct has ceased and such confirmation has been accepted by the notifying Party.

16.5 If the Controller objects to the Processor's engagement of a new Sub-processor pursuant to Clause 12.7 of this DPA, the Controller shall have the right to terminate this DPA with immediate effect.

17 Measures upon Termination of the DPA

17.1 Upon termination of this DPA, the Processor shall, without undue delay and at the Controller's choice, either erase and certify to the Controller that such erasure has been completed, or return:

- a) all Personal Data processed on behalf of the Controller; and
- b) all related information such as Logs, Instructions, system solutions, descriptions and other documentation received by the Processor through the exchange of information under this DPA.

17.2 In connection with the return of Personal Data, the Processor shall also erase any existing copies of Personal Data and related information, including Personal Data contained in backups.

17.3 The obligation to erase or return Personal Data or related information shall not apply where storage of the Personal Data or information is required by Union law or applicable national law under which Processing may be carried out pursuant to this DPA.

17.4 Where Personal Data or related information is returned, it shall be provided in a commonly used and standardized format, unless the Parties have agreed on another format.

17.5 Until such time as the Personal Data and related information have been erased or returned, the Processor shall continue to ensure compliance with this DPA.

17.6 Erasure or return pursuant to this DPA shall be completed no later than thirty (30) calendar days from the date of termination of the DPA, unless otherwise specified in the Instructions. Any Processing of Personal Data carried out by the Processor thereafter shall be considered unauthorized Processing.

17.7 The confidentiality obligations set out in Section 8 shall continue to apply notwithstanding the termination of this DPA.

18 Notices under this DPA and Instructions

18.1 Notices relating to this DPA and its administration, including termination, shall be sent by email or by any other method agreed between the Parties to the designated contact person for this DPA of the respective Party.

18.2 Notices relating to the Parties' cooperation on data protection matters concerning the Processing shall be sent by email or by any other method agreed between the Parties to the designated contact person for the Parties' data protection cooperation.

18.3 A notice shall be deemed to have been received no later than one (1) Business Day after it has been sent.

19 Contact Persons

19.1 Each Party shall appoint a contact person for this DPA.

19.2 Each Party shall appoint a contact person for the Parties' cooperation on data protection matters.

20 Responsibility for Party Information and Contact Details

20.1 Each Party shall be responsible for ensuring that the information set out in Section 1 of this DPA is accurate and up to date at all times.

20.2 Any changes to the information set out in Section 1 shall be notified to the other Party in accordance with Clause 18.1 of this DPA.

21 Dispute Resolution

21.1 This DPA shall be governed by and construed in accordance with the laws of Sweden, excluding its conflict of laws rules. Any disputes arising out of or in connection with this DPA shall be settled by a competent Swedish court.

22 Execution of the DPA

22.1 This DPA is made available either in digital form for electronic signature or in paper form for handwritten signature. In the latter case, the DPA shall be executed in two (2) counterparts, each Party receiving one copy.

22.2 If this DPA is signed electronically, the signature blocks below shall not apply.

Appendix 1 Controller's Instructions for the Processing of Personal Data

[Gulmarkerad text inom hakparenteser tas bort inför att Personuppgiftsbiträdesavtal upprättas.]

[Om Personuppgiftsbiträdet ska utföra flera Behandlingar av Personuppgifter åt den Personuppgiftsansvarige för olika ändamål, t.ex. dels tillhandahålla ett IT-system, dels tillhandahålla support och service avseende systemet, ska en Instruktion per ändamål upprättas.]

In addition to what is already set out in the Data Processing Agreement, the Processor shall also comply with the following Instruction:

1. Purpose, Subject Matter and Nature of the Processing	1 a. The subject matter of the Processor's Processing of Personal Data on behalf of the Controller is: [Provide a general description of the main purpose of the Processor's Processing of Personal Data on behalf of the Controller, e.g. provision of an HR tool for payroll administration, a cloud service for storage of operational data, or a system for monitoring access to office premises.] 1 b. The purpose of the Processor's Processing of Personal Data on behalf of the Controller is: [Specify the purpose of the Processing, i.e. why the Processor is to Process the Personal Data on behalf of the Controller – what is the objective of the Processing? Examples of purposes include administering payment of salaries and other employee benefits, storing information assets in a secure and cost-efficient manner, or preventing unauthorized access to office premises. The description shall be sufficiently detailed to enable external parties (e.g. a supervisory authority) to understand the content and risks associated with the Processing entrusted to the Processor.] 1 c. The Processor's Processing of Personal Data on behalf of the Controller primarily comprises the following processing activities (nature of the Processing): ☐Collection ☐Recording ☐Organization, structuring ☐Storage ☐Adaptation/alteration ☐Erasure ☐Consultation (access/reading) ☐Disclosure by transmission ☐Other:
2. The Processing concerns the following categories of Personal Data:	The Processor is authorized to process the following types of Personal Data on behalf of the Controller: [Specify the types of Personal Data that the Processor is authorized to process on behalf of the Controller, e.g. name, email address, postal address, telephone number, membership number, IP address, images, video recordings, health data, etc.]
3. The Processing concerns the following categories of Data Subjects:	The Processor is authorized to Process Personal Data relating to the following categories of Data Subjects: [Specify the categories of Data Subjects whose Personal Data the Processor is authorized to process, e.g. employees, consultants, passengers, children, etc.] ☐ Employees ☐ Customers ☐ Suppliers ☐ Passengers ☐ Visitors ☐ Next of kin ☐ Consultants ☐ Other (specify groups): _____



4. Specific handling requirements relating to the Processing of Personal Data carried out by the Processor	The Processor shall comply with the following specific handling requirements when Processing Personal Data on behalf of the Controller: [Examples of such requirements include that Personal Data shall be erased after a specified retention period, that backup copies shall not be retained beyond a specified period, or that specific procedures for access management shall be implemented. Requirements relating to logging, encryption, segregation of data, or restrictions on remote access may also be specified here.]
5. Specific technical and organizational security measures applicable to the Processor's Processing of Personal Data	The Processor shall implement the following security measures in connection with the Processing of Personal Data: [If information security and cybersecurity requirements are set out in a separate agreement, refer to the relevant appendix.] <u>Specific requirements relating to Logging:</u>
6. Location and Transfer of Personal Data to a Third Country	The Processor shall comply with the following requirements regarding the location of Personal Data. The Processor is only authorized to process the Personal Data at the following location(s): [Specify the location(s) of the Processing (postal address, country).] If the Controller has not provided Instructions permitting the transfer of Personal Data to a Third Country, the Processor shall not be entitled to carry out such transfer. The Processor shall comply with the following requirements regarding transfers of Personal Data to a Third Country: The Processor shall ensure that a valid transfer mechanism pursuant to Chapter V of the GDPR is in place. The Processor shall be responsible for implementing, where necessary, supplementary measures in accordance with the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data. See further instructions in <i>Appendix 3 – Description of Transfers to Third Countries</i>.
7. Duration of the Processing	[Specify the period of time, or the criteria used to determine the period, during which the Processor is authorized to Process Personal Data on behalf of the Controller. For example, reference may be made to the term of the Data Processing Agreement.]
8. Other Instructions concerning the Processing of Personal Data carried out by the Processor	[Add, where necessary, any additional Instructions relating to the Processor's Processing of Personal Data on behalf of the Controller beyond those set out above. Such Instructions may, for example, concern the procedure for the Controller's audits and inspections of the Processor's Processing of Personal Data pursuant to Section 9 of the DPA.]

Appendix 2 List of Approved Sub-processors

☐	There are no Processors at the time of execution of the agreement.
--------------------------	---

The Controller hereby approves that the Processor engages the following Sub-processors for the Processing of Personal Data.

1	Sub-processor's name and corporate registration number	[Specify the organization's full legal name] [Specify the organization's corporate registration number]
	Address and contact details	[Specify the Sub-processor's postal address and the name, telephone number and e-mail address of the contact person.]
	Location of Personal Data (address, country)	[Specify where the Sub-Processor Processes the Personal Data.]
	Types of Personal Data Processed by the Processor	[Specify which types of Personal Data the Sub-Processor is authorized to Process, e.g. name, e-mail address, postal address, telephone number, membership number, IP address, images, moving images, health data, etc.]
	Type of data	☐ Plain text ☐ Pseudonymized ☐ Encrypted
	Purpose of the Sub-Processor's Processing	[Specify the purpose of the Processing, i.e. why the Sub-Processor is to Process the Personal Data on behalf of the Controller – what is the purpose of the Processing?]
	Processing period	[Specify the period during which the Sub-Processor's Processing takes place]

2	Sub-processor's name and corporate registration number	[Specify the organization's full legal name] [Specify the organization's corporate registration number]
	Address and contact details	[Specify the Sub-processor's postal address and the name, telephone number and e-mail address of the contact person.]
	Location of Personal Data (address, country)	[Specify where the Sub-Processor Processes the Personal Data.]
	Types of Personal Data Processed by the Processor	[Specify which types of Personal Data the Sub-Processor is authorized to Process, e.g. name, e-mail address, postal address,

		telephone number, membership number, IP address, images, moving images, health data, etc.]
	Type of data	☐ Plain text ☐ Pseudonymized ☐ Encrypted
	Purpose of the Sub-Processor's Processing	[Specify the purpose of the Processing, i.e. why the Sub-Processor is to Process the Personal Data on behalf of the Controller – what is the purpose of the Processing?]
	Processing period	[Specify the period during which the Sub-Processor's Processing takes place]

Appendix 3 – Description of transfer to third countries

[Om flertal överföringar förekommer ska en Redogörelse per överföring upprättas.] [If multiple transfers occur, a separate description shall be prepared for each transfer.]

[Specify the organization's full legal name] [Specify the organization's corporate registration number] [Specify location(s) for the Processing (postal address, country).]	
Transfer of Personal Data to a Third Country occurs when Personal Data are made available to someone (a service provider or its sub-contractor) in a country outside the EU/EEA	
☐	Personal Data are not transferred to a Third Country.
☐	Personal Data are transferred to a Third Country <i>Transfer of Personal Data to a Third Country or an international organization is permitted only if one or more of the transfer grounds set out below are fulfilled (tick one or more).</i>
☐	The transfer takes place to a Third Country or an international organization that has been assessed by the European Commission as providing an adequate level of protection:
	☐ Andorra, Argentina, Bailiwick of Guernsey, Faroe Islands, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay ☐ Canada: where its legislation for the protection of Personal Data in the private sector is applicable to the recipient's Processing of Personal Data. ☐ United States, provided that the recipient is covered by the EU–U.S. Data Privacy Framework.
☐	Appropriate safeguards have been implemented in accordance with the following:
	☐ Binding Corporate Rules (BCR). <i>Specify which Binding Corporate Rules:</i>
	☐ Standard Contractual Clauses (SCC) – adopted by the European Commission. Attach these where applicable. ☐ An approved code of conduct , specify which: ☐ An approved certification mechanism , specify which:
	☐ A legally binding and enforceable instrument – applicable only between public authorities. ☐ Authorization for the transfer from the supervisory authority.
☐	The Data Subject has explicitly consented thereto, after having been informed of the risks associated with transfers carried out in the absence of an adequacy decision or appropriate safeguards.
☐	Other specific situations and occasional transfers.