

Itm8 Sverige AB

---

# The Data Processing Agreement

# Table of contents

1	Standard contractual clauses	2
2	Preamble	3
3	The rights and obligations of the data controller	4
4	The data processor acts according to instructions	4
5	Confidentiality	4
6	Security of processing	5
7	Use of sub-processors	5
8	Transfer of data to third countries or international organisations	6
9	Assistance to the data controller	7
10	Notification of personal data breach	8
11	Erasure and return of data	9
12	Audit and inspection	9
13	The parties' agreement on other terms	9
14	Commencement and termination	9
15	Data controller and data processor contacts	10
	Appendix A - Information about the processing	11
	Appendix B - Sub-processors	12
	Appendix C - Instructions pertaining the processing of personal data	13
	Appendix D – The parties' terms of agreement on other subjects	16

## Data processing agreement clauses

### 1 Standard contractual clauses

Pursuant to Article 28(3) of Regulation 2016/679 (General Data Protection Regulation) with regard to the processing of personal data by the data processor

between

Customer (specified in the Service Agreement)

(hereinafter "the data controller")

and

itm8 company (specified in the Service Agreement)

(hereinafter the "data processor"),

each of which is a "party" and together constitute the "parties"

the following standard contractual clauses (the "Clauses") have been agreed in order to comply with the GDPR and to ensure the protection of the privacy and fundamental rights and freedoms of natural persons.

## 2 Preamble

1. The Customer has entered into an Agreement ("**Service Agreement**") with the Supplier and the performance of the agreed Services ("**Services**") is subject to these Conditions.
2. These Clauses relate to the processing activity(ies) ("**Processing Activity**") agreed in the Service Agreement.
3. In connection with the provision of Services, the data processor processes personal data on behalf of the data controller, which is why the parties have entered into this Data Processing Agreement and its appendices (collectively the "Data Processing Agreement"), which forms an integral part of the parties' Service Agreement.
4. These Clauses set out the rights and obligations of the data processor when processing personal data on behalf of the data controller.
5. These Clauses are designed to enable the parties to comply with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
6. The Clauses take precedence over any corresponding clauses in other agreements between the parties.
7. These Clauses are accompanied by appendices and the appendices form an integral part of the Clauses.
8. Appendix A contains details of the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing. [Appendix A1](#) contains requirements for the agreed Processing Activities associated with the agreed Service Area(s).
9. Appendix B contains the data controller's conditions for the data processor's use of sub-processors. [Appendix B1](#) contains a list of sub-processors for the Processing Activities related to the agreed Service Area(s) that the data controller has authorised the use of.
10. Appendix C contains the data controller's instructions regarding the data processor's processing of personal data, a description of the security measures that the data processor must implement as a minimum, and how the data processor and any sub-processors are supervised. [Appendix C1](#) contains the agreed security measures.
11. Appendix D contains clauses relating to other activities not covered by the Clauses, including separate national data protection requirements described in [Appendix D8](#).
12. The clauses and their appendices are stored electronically at [Legal & Compliance in itm8](#). The data controller undertakes to keep its own copy of the Clauses including appendices.

13. These Clauses do not release the data processor from obligations imposed on the data processor under the General Data Protection Regulation or any other mandatory legislation.

### **3 The rights and obligations of the data controller**

1. The data controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24 of the Regulation), the applicable EU or Member state<sup>1</sup> data provisions and the Clauses.
2. The data controller has the right and obligation to decide for which purpose(s) and with which means personal data may be processed.
3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

### **4 The data processor acts according to instructions**

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by EU or Member State law to which the data processor is subject. This instruction shall be specified in Appendix A and [Appendix A1](#) and Appendix C and [Appendix C1](#). Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with these Clauses.
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member state data protection provisions.

### **5 Confidentiality**

1. The data processor shall only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's instructions, who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons to whom access has been granted shall be kept under periodic review. Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned duty of confidentiality.

---

<sup>1</sup> References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

## 6 Security of processing

1. Article 32 GDPR states that the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risks, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- a. 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 availability and access to personal data in a timely manner in the event of a physical or technical incident.
  - d. a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.
2. According to Article 32 GDPR, the data processor shall also - independently from the data controller - evaluate the risks to the rights of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
  3. Furthermore, the data processor shall assist the data controller in its compliance with the data controller's obligation under Article 32 GDPR, inter alia, providing the data controller with the necessary information regarding the technical and organisational security measures already implemented by the data processor pursuant to Article 32 GDPR and any other information necessary for the data controller to comply with its obligation under Article 32 GDPR.

If addressing the identified risks - in the data controller's assessment - requires the implementation of additional measures beyond the measures already implemented by the data processor, the data controller shall specify the additional measures to be implemented in Appendix C including [Appendix C1](#).

## 7 Use of sub-processors

1. The data processor must fulfil the conditions referred to in Article 28(2) and (4) GDPR in order to use engage another processor (a sub-processor).
2. The data processor shall therefore not engage a sub-processor to fulfil these Clauses without prior general written approval from the data controller.

3. The data processor has the data controller's general authorisation to engage sub-processors as stated in [Appendix B1](#).
4. [Appendix B1](#) contains a list of sub-processors for the agreed Processing Activities that are linked to the agreed Service Area(s) that the data controller has authorised the use of.
5. The data processor shall notify the data controller in writing of any planned changes regarding the addition or replacement of sub-processors with at least 30 days' notice, thereby giving the data controller the opportunity to object to such changes prior to the use of the sub-processor(s) in question. The list of sub-processors already authorised by the data controller is set out in [Appendix B1](#).
6. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the data processor shall, by contract or other legal act under EU or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Clauses, in particular providing appropriate guarantees that the sub-processor will implement the technical and organisational measures in such a manner that the processing complies with the requirements of these Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7. The sub-processor agreement(s) and any subsequent amendments thereto shall - at the request of the data controller - be sent a copy to the data controller, which thereby has the opportunity to ensure that similar data protection obligations arising from these Clauses are imposed on the sub-processor. Clauses on commercial terms that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
8. If the sub-processor does not fulfil its data protection obligations, the data processor remains fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 92 GDPR – against the data controller and the data processor, including the sub-processor.

## **8 Transfer of data to third countries or international organisations**

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor may not, within the framework of the Clauses:
  - a. transfer personal data to a data controller or a data processor in a third country or an international organisation.
  - b. transfer the processing of personal data to a sub-processor in a third country.
  - c. process personal data in a third country.
4. The data controller's instructions regarding the transfer of personal data to a third country, including, if applicable, the transfer basis in Chapter V GDPR on which the transfer is based, shall be specified in Appendix C.6.
5. These Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and these Clauses shall not constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

## 9 Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor must, insofar as this is possible, assist the data controller in the data controller's compliance with:

- a. the right to be informed when collecting personal data from the data subject.
- b. the right to be informed when personal data have not been obtained from the data subject.
- c. the right of access by the data subject.
- d. the right to rectification.
- e. the right to erasure ("the right to be forgotten").
- f. the right to restriction of processing.
- g. notification obligation regarding rectification or erasure of personal data or restriction of processing.
- h. the right to data portability.
- i. the right to object.
- j. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3, the data processor shall, taking into account the nature of the processing and the information available to the data processor, further assist the data controller with:
  - a. the data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Swedish Data Protection Agency (Integritetsmyndigheten, "IMY"), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
  - b. the data controller's obligation to without undue delay notify the personal data breach to the data subject, when the breach is likely to result in a high risk to the rights and freedoms of natural persons.
  - c. the data controller's obligation to carry out an assessment of the impact of the intended processing activities on the protection of personal data prior to processing (a data protection impact assessment).
  - d. the data controller's obligation to consult the competent supervisory authority, the Swedish Data Protection Agency, IMY, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.
3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clauses 9.1 and 9.2.

## 10 Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after becoming aware of the breach so that the data controller can fulfil its obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
3. In accordance with Clause 9.2.a, the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority. This means that the data processor shall assist in providing the following information, which, according to Article 33(3) GDPR, shall be included in the data controller's notification of the breach to the competent supervisory authority:
  - a. 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. the likely consequences of the personal data breach.

- c. the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where applicable, measures to mitigate its possible adverse effects.
4. The parties shall define in Appendix C the information to be provided by the data processor in the context of its assistance to the data controller in its obligation to notify personal data breaches to the competent supervisory authority.

## **11 Erasure and return of data**

1. Upon termination of the personal data processing services, the data processor shall be under the obligation to delete all personal data processed on behalf of the data controller and confirm to the data controller that the data has been erased or return all personal data and delete existing copies, unless EU or Member State law requires the storage of the personal data.

## **12 Audit and inspection**

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in Appendices C.7 and C.8.
3. The data processor shall be required to provide supervisory authorities, which pursuant to applicable legislation have access to the data controller's or data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

## **13 The parties' agreement on other terms**

1. The parties may, in the agreement for the delivery of Services or in Appendix D, agree other clauses regarding the processing of personal data, e.g. on liability, as long as they do not directly or indirectly contradict the Clauses or prejudice the data subject's fundamental rights and freedoms under the GDPR.

## **14 Commencement and termination**

1. The Clauses shall become effective on the date of the Parties' accession to the Service Agreement.
2. Both parties shall be entitled to require the Clauses renegotiated if changes in legislation or inexpediencies in the Clauses give rise to such.
3. The Clauses shall apply for the duration of the provision of personal data processing services. During this period, the Clauses cannot be terminated unless other Clauses

governing the provision of the personal data processing services have been agreed between the parties.

4. If the provision of Services relating to the processing of personal data ceases and the personal data has been deleted or returned to the data controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated with written notice by either party.
5. Signature
  - a. The Clauses are considered accepted in connection with the signing of the parties' Service Agreement regarding the delivery of Services.
  - b. The parties acknowledge and agree that a digital signature provided by a party in connection with the conclusion of the Service Agreement has the same legal validity and binding effect as a handwritten (physical) signature of the clauses.

## **15 Data controller and data processor contacts**

1. The parties may contact each other via the contact persons specified in the agreed Service Agreement.
2. The parties are obliged to keep each other informed of changes regarding contact persons.

## Appendix A - Information about the processing

### A.1 Purpose of the data processor's processing of personal data on behalf of the data controller

The parties have agreed that the data processor shall provide any agreed Service regulated in the parties' Service Agreement. The performance of the agreed Services involves a Processing Activity in terms of data protection law. The agreed Processing Activities are set out in the Service Agreement.

The agreed Processing Activities related to the agreed Service Areas determine the requirements for the Customer's instructions, the subject matter of the processing, the nature of the processing, types of personal data about the data subjects and types of data subjects described in [Appendix A1](#).

The data processor's processing of personal data on behalf of the data controller commences after the parties' agreement regarding the provision of Services enters into force and until it ceases.

## Appendix B - Sub-processors

### B.1. Sub-processors utilised

Upon commencement of the Clauses, the data controller has authorised the engagement of sub-processors for the agreed Processing Activities related to the agreed Service Area(s).

[Appendix B1](#) lists the sub-processors for the agreed Processing Activities associated with the agreed Service Area(s).

When purchasing or changing Service Areas, the regulation of authorised sub-processors will appear in [Appendix B1](#).

The data processor's notification of planned changes regarding the addition or replacement of sub-processors is made as described in B.2.

### B.2 Prior notice for authorisation of sub-processors

The data processor's notification of any planned changes regarding the addition or replacement of sub-processors must be received by the data controller at least 30 days before the application or change is to take effect, as far as this is immediately possible.

Notwithstanding the above, the data controller accepts that there may be special cases where there may be a specific need for the change regarding the addition or replacement of sub-processors to be made at shorter notice or immediately. In such cases, the data processor will notify the data controller of the change as soon as possible.

If the data controller objects to the changes, the data controller shall notify the data processor before the notified effective date of the change. The data controller may only object if the data controller has reasonable, concrete reasons to do so.

By the data controller's objection, the data controller also accepts that the data processor may be prevented from providing all or part of the agreed services. Such non-fulfilment shall not be attributable to the data processor's breach. The data processor maintains its claim for payment for such services, notwithstanding that they cannot be provided to the data controller.

Where it is specifically agreed that the data processor may not use sub-processors without the data controller's prior authorisation, the data controller accepts that this may result in the data processor being prevented from performing Services. Therefore, if the data controller has refused to allow changes to be made regarding the addition or replacement of sub-processors, failure to provide services will not be considered a breach of the parties' agreement regarding the provision of Services attributable to the data processor in cases where the non-performance is attributable to a sub-processor.

## Appendix C - Instructions pertaining the processing of personal data

### C.1. The subject of/instruction for the processing

The data controller instructs the data processor to process personal data in accordance with what has been agreed between the parties, where the data processor's security measures are described in [Appendix C1](#).

### C.2 Security of processing

The agreed security measures are stated in [Appendix C1](#).

### C.3 Assistance to the data controller

The data processor shall - insofar as possible - within the scope and extent set out below - assist the data controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

At the specific request of the data controller and taking into account the nature of the processing, the data processor shall, as far as possible, assist the data controller by means of appropriate technical and organisational measures to fulfil the data controller's obligation to respond to requests for exercising the rights of data subjects as laid down in the GDPR.

If a data subject submits a request for the exercise of his or her rights to the data processor, the data processor shall inform the data controller without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor shall, upon specific request, also assist the data controller in ensuring compliance with the data controller's obligations in relation to:

- Implementation of appropriate technical and organisational measures
- Security breaches
- Notification of personal data breaches to the data subject
- Conducting impact assessments
- Prior consultation with regulatory authorities

### C.4. Storage period/erasure procedures

Upon termination of the personal data processing service, the data processor shall either delete or return the personal data in accordance with clause 11.1.

### C.5 Processing location

Processing of the personal data covered by the Clauses may not, without the prior written authorisation of the data controller, take place at locations other than one or more of the following addresses:

- Addresses of the data processor.
- Data centers that the data processor uses.
- Sub-processors and their sub-processors' addresses.

In addition, remote work may be performed in accordance with the data processor's guidelines for remote work.

## **C.6. Instruction on the transfer of personal data to third countries**

The data processor may only transfer personal data to countries outside the EU or EEA (a "Third Country") or international organisation as described below.

### C.6.1 General authorisation for the transfer of personal data to secure Third Countries

The data controller gives its general and prior authorisation (instruction) under the Clauses for the data processor to transfer personal data to third countries if the European Commission has determined that the third country, territory or sector concerned has an adequate level of protection.

The data controller also gives its general and prior consent (instruction) under the Clauses for the data processor to transfer personal data to organisations in the United States certified under the EU-U.S. Data Privacy Framework ("DPF").

### C.6.2 Authorisation of transfer to specific recipients of personal data in third countries

The data controller shall instruct the data processor to transfer personal data to Third Countries using the specified sub-processors where there is a transfer of personal data to Third Countries as specified in [Appendix B1](#). Furthermore, the data processor shall be authorised to transfer personal data to Third Countries when this is required by the data controller's actions.

The data processor is entitled to secure the necessary transfer basis, e.g. by using the Standard Contractual Clauses (SCC) and thereby entering into Standard Contractual Clauses with the relevant sub-processor. The data controller shall, to the extent necessary, assist the processor in securing the transfer basis, including e.g. Standard Contractual Clauses.

In the event that the European Commission adopts new Standard Contractual Clauses after the conclusion of the agreement, the data processor is authorised to renew, update and/or use the Standard Contractual Clauses in force at any time.

The content of these clauses shall not be deemed to modify the content of the Standard Contractual Clauses.

If the data controller does not provide documented instructions in these Clauses or subsequently regarding the transfer of personal data to a third country, the data processor is not authorised to make such transfers within the framework of these Clauses.

## **C.7 Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor**

Under Articles 24 and 28 GDPR, the data controller has the right and obligation to supervise the data processor's processing of personal data on behalf of the data controller. The data controller's implementation of supervision of the data processor can be done by the data controller performing one of the following actions:

- self-monitoring based on documents that the data processor makes available to the data controller,
- written supervision or
- physical inspections.

#### C.7.1 Self-monitoring

The data controller conducts self-monitoring of the data processor based on documents made available on [Legal & Compliance in itm8](#).

#### C.7.2 Written supervision and physical inspection

The data controller may choose to carry out an audit either as a written audit or by physical inspection. The audit can be carried out by the data controller itself and/or in co-operation with a third party. An audit must be based on the security measures agreed between the parties.

When requesting a written or physical inspection, please follow the procedure below.

Procedure and reporting for written supervision or physical inspection:

- The data controller sends their supervision form to the data processor via email to [gdpr@itm8.dk](mailto:gdpr@itm8.dk) with a request for supervision and/or inspection.
- The data processor confirms receipt and states the final date of the audit and/or inspection.
- The implementation of the audit and/or inspection takes place.
- The data controller will forward any observations from the audit to [gdpr@itm8.dk](mailto:gdpr@itm8.dk).
- The data processor reviews and comments on any observations made by the data controller (may be repeated several times).
- The data controller performs its final conclusion of the audit and sends the report to the data processor.
- The inspection is finalised.

### **C.8 Procedures for audits, including inspections, of processing of personal data being performed by to sub-processors**

Based on the data processor's risk assessment and taking into account the specific processing activities, the data processor performs audits, including inspections, of sub-processors' processing of personal data either in the form of self-monitoring of audit statements and similar (where possible), written supervision or physical inspection, or a combination thereof.

The data controller may, at the data controller's request, obtain further information on the control measures implemented and applied to each sub-processor.

## Appendix D – The parties' terms of agreement on other subjects

### D.1 General

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the following additional terms.

The Clauses of this agreement take precedence over any corresponding regulation in Service Agreements between the parties regarding the part of the data processor's activities and responsibilities related to data processing, while the performance of all other activities related to the delivery of agreed Services is subject to the other parts of the Service Agreement.

The other terms of the Service Agreement, including limitations of liability, etc. also apply to the data processor's fulfilment of these Clauses.

In the event of any inconsistency between the Clauses and the terms set out in this Appendix D, Appendix D shall prevail, and if the Service Agreement otherwise contains terms on the data processor's processing activities, Appendix D shall also prevail.

### D.2 Consequences of the data controller's unlawful instruction

The data controller is aware that the data processor is dependent on the data controller's instructions on the extent to which the data processor is authorised to use and process the personal data on behalf of the data controller. The data processor is therefore not liable for claims arising from the data processor's acts or omissions to the extent that these acts or omissions are a data processing activity carried out in accordance with the data controller's instructions.

### D.3 Implementation of other security measures

The data processor is entitled to implement and maintain alternative security measures to those specified in the agreement for the delivery of Services and [Appendix C1](#), provided that such alternative security measures overall ensure a level of security equivalent to the prescribed security measures.

### D.4 Use of Third-Party Services

Notwithstanding clause 7 of the Clauses, it is agreed that if the data processor uses sub-processors identified in a Service Agreement as a provider of Standard Third-Party Services, any processing activities of Third-Party Suppliers (as a sub-processor) in connection with the provision of these Standard Third-Party Services will be subject to the Third-Party Supplier's own terms for the processing activities as sub-processor.

The data processor has made the terms and conditions available on [Legal & Compliance in itm8](#) and it is the data controller's own responsibility to familiarise itself with them and otherwise ensure that these terms and conditions satisfactorily meet the requirements for the Third-Party Supplier's processing activities.

The data controller is aware that these terms and conditions may be changed by the individual Third-Party Supplier on an ongoing basis, and the data controller must thus continuously ensure that these fulfil the requirements for the processing activities.

The data controller may contact the data processor at any time in order to obtain the terms and conditions.

By accepting the Clauses, the data controller also accepts and instructs that processing activities are carried out on the terms of the Third-Party Supplier.

#### **D.5 Erasure and return of data**

It is agreed between the parties that the data controller will instruct the data processor to delete and return the personal data in connection with the termination of the Clauses.

The data controller shall, no later than 30 days after the processing of personal data has ceased, notify the data processor whether all personal data shall be erased or returned to the data controller. In the event that personal data is to be returned to the data controller, the data processor must also delete any copies. The data processor must ensure that any sub-processors also comply with the notice from the data controller.

The erasure obligation does not apply to (i) copies of electronically exchanged personal data stored as part of automated backup functions, provided that access is restricted to IT or compliance personnel and provided that such data continues to be processed in accordance with the Clauses, and (ii) personal data that must be retained by the data processor under mandatory law.

If the data processor has not received notification from the data controller within 30 days after the processing of personal data has ceased, the data processor shall send a reminder to the data controller. If the data controller does not subsequently notify the data processor whether all personal data is to be erased or returned to the data controller, the data processor is entitled to erase personal data without further notice.

The data processor is entitled to remuneration for its processing activities until such time as the data controller notifies the data processor whether all personal data is to be erased or returned to the data controller.

#### **D.6 Remuneration**

##### D.6.1 Assistance - general

Unless the data processor, as part of the agreed Services and within the fixed fee for such Services, has undertaken to fulfil the Clauses, the data processor will be entitled to remuneration for assistance according to the assistance services agreed in the Clauses, including clause 9.

The remuneration is calculated on the basis of the labour time spent and the agreed hourly rates in the Service Agreement for the provision of Services, and if no hourly rates have been agreed herein, then according to the data processor's applicable hourly rates.

Any external costs incurred, including costs incurred by the data processor for the assistance of sub-processors, shall be invoiced to the data controller.

#### D.6.2 Implementation of other security measures

If the data controller's instructions etc. and the data processor's ongoing assessments in general result in more stringent requirements for the requirements contained in a Service Agreement for security measures regarding the provision of Services or for Appendix C and [Appendix C1](#), the data processor will loyally endeavour to meet such requirements if this is technically possible and compatible with the fulfilment of other requirements for the affected Services.

The data processor is entitled to remuneration and cost recovery according to the same principles as above.

#### D.6.3 Monitoring and auditing

The data processor is entitled to remuneration for the data controller's performance of supervision and auditing. The remuneration is calculated on the basis of the working hours spent and the agreed hourly rates in the Service Agreement for the provision of Services, and if no hourly rates have been agreed herein, then according to the data processor's applicable hourly rates.

Any external costs incurred, including costs incurred by the data processor for the assistance of sub-processors, shall be invoiced to the data controller.

### **D.7 Liability and breach**

Any breach of the Clauses shall be governed by and dealt with in accordance with the parties' Service Agreement regarding the provision of Services, with the following additions;

- a) a) Where the data processor has paid compensation to data subjects in accordance with Article 82 of the General Data Protection Regulation (GDPR) or the Swedish Liability Act (Skadeståndslagen (1972:207), "SkL"), the data processor shall have full right of recourse against the data controller for the portion of such compensation exceeding the agreed limitation of liability set out in the parties' Service Agreement relating to the provision of the Services. The parties hereby contractually derogate from Article 82(5) GDPR and the Swedish Liability Act (Skadeståndslagen (1972:207)).
- b) Notwithstanding Article 82(5) GDPR, if the data processor has paid compensation to an injured party that does not correspond to full compensation, the data processor may have recourse according to the principle in Article 82(5).
- c) In relation to other compensation for non-pecuniary losses to data subjects, the principle of Article 82 shall also apply with regard to the internal final allocation of responsibilities between the data processor and the data controller.
- d) The Parties may not claim recourse or damages from the other Party for administrative fines or other public law sanctions imposed pursuant to the General Data Protection Regulation (GDPR), including administrative fines under Article 83 GDPR, or pursuant to applicable Swedish data protection legislation.
- e) The data processor's total liability for breach of the Clauses is subject to the limitation of amount (and included in the maximisation of damages) that may result from the parties' Service Agreement. The liability (including any damages or other financial compensation

that may have been granted to the data controller under the Service Agreement) shall be limited to an amount lower than 150% of the amount received by the data processor in the 12 months preceding the harmful act. If a 12-month period has not elapsed, the limitation of liability is calculated as the average of the amounts received in the months that have elapsed multiplied by 12.

- f) The data processor's liability for breach of the Clauses does not include indirect loss, including operating loss, consequential damage or other indirect loss.
- g) The data processor is not liable for breach of the Clauses caused by computer viruses, cybercrime or other forms of unauthorised interference by third parties in the data controller or the data processor's IT systems, unless the loss is directly related to failure to meet agreed security requirements in the parties' Service Agreement.

#### **D.8 National special regulations**

If the data controller is located outside Sweden, separate requirements apply which are in accordance with national data protection regulations in the data controller's home country. The national special regulations can be found here: [Appendix D8](#).