itm8®

Itm8 | Improsec A/S

Data Processing Agreement

Standalone

Table of Contents

Data processing agreement

1. Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[Firma]

(the data controller)

and

itm8 | Improsec A/S

CVR 37292451

(the data processor)

each referred to as a "party" and collectively as the "parties"

the following Standard Contractual Clauses (the "Clauses") have been agreed in order to comply with the General Data Protection Regulation and to ensure the protection of privacy and fundamental rights and freedoms of individuals.

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the Clauses of services comprised by the parties' agreement(s) regarding IT Services (the "Service Agreement", the "Service" and/or the "Services"), the data processor will process personal data on behalf of the data controller in accordance with the Clauses. The Clauses may cover the data processor's processing activities under several independent Service agreements entered into between the parties.

4. Four appendices are attached to the Clauses and form an integral part of the Clauses.

5. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

6. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

7. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

8. Appendix D contains supplemental the Clauses.

9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other essential legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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 Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. 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 the 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 the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of 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 confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   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 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.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms 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 ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided as a deviation in Appendix D.8. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the 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.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain 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 82 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 therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor 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 tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V 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 shall, 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 furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance 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, Danish Data Protection Agency, 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 communicate the personal data breach to the data subject, when the personal data 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 envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, Danish Data Protection Agency, 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 Clause 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 the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's 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, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data 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 controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires 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 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 the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and 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 parties' agreement regarding the data processor's provision of the Services ("Services Agreement") or in Appendix D, agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing Services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing Services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

   Name NAME
   Position POSITION

   Signature _____

   On behalf of the data processor

   Name NAME
   Position POSITION

   Signature _____

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points

THE DATA CONTROLLER		THE DATA PROCESSOR	
Name:	Name	Navn:	Improsec Security
E-mail:	E-mail adresse	Mail:	gdpr@improsec.com
Tel.:	Phone	Tlf.:	+45 53 57 53 37

Appendix A – Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller

The parties have agreed that the data processor will provide the following services:

SELECTED (X)	PURPOSE OF THE PROCESSING
☐	Consultancy Services

A.1.1 Consultancy Services

The purpose of the processing is to carry out specifically agreed consultancy tasks. Consequently, the purpose will vary, but will always be related to an agreed consultancy task.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing)

A.2.1 Consultancy Services

The data processor will carry out specific and limited tasks. Consultancy tasks are carried out in the data controller's systems and with the data controller's data, and the processing will be defined for each specific task.

Tasks are requested and defined by the data controller, and the data processor will assist to the extent required in order to ensure a proper definition of tasks.

A.3. The processing includes the following types of personal data about data subjects

General personal data (cf. Article 6 of the General Data Protection Regulation):

☒ Name

☒ Address

☒ Email

☒ Phone number

☒ Financial information

☐ Other personal data as specified

... Specify other categories

Sensitive personal data (cf. Article 9 of the General Data Protection Regulation):

☒Racial or ethnic background.

☒ Political opinion.

☒ Religious beliefs.

☒ Philosophical beliefs.

☒ Trade union membership.

☒ Health issues, including abuse of medicine, narcotics, alcohol, etc.

☒ Sexual matters.

Information about the private life of individuals (cf. Article 8 of the Danish Data Protection Act):

☒ Criminal matters.

☒ Relevant social problems.

Other information about purely private matters not mentioned above:

☒ Other private matters.

Information about National Identification Number (CPR) (cf. Article 11 of the Danish Data Protection Act):

☒ National Identification numbers (CPR).

A.4. The processing includes the following categories of data subjects

Categories of data subjects, identified or identifiable natural persons comprised by the data processor's processing:

☒Employees

☒ Children

☒ The data controller's own customers

☐ Other categories as specified.

... Specify other categories

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence.

The data processor's processing of personal data on behalf of the data controller is performed when the parties' Service Agreement comes into force and will continue until the Service Agreement is terminated.

Appendix B – Authorised Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller has approved the engagement of sub-processors described in the parties' agreement regarding the data processor's provision of Services to the data controller for the described processing activity.

NAME	COMPANY NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Ireland Operations, Ltd. South County Business Park Leopardstown	SE-no.: IE8256796U	Data is stored within the EU, but support can be provided from around the world	Microsoft O365 and Azure

The list of sub-processors used at the time of contracting is inserted in the above table and will be adjusted in case of acquisition or changes in services.

After commencement of the Clauses, the data processor can use other sub-processors. The data controller will be informed of changes in data processors used upon purchase of new services or data processor changes to services. In addition, an appendix of currently used sub-processors can be provided upon request.

The procedure for the data processor's notice regarding planned changes in terms of addition or replacement of sub-processors is described in clause B.2.

B.2. Notice for approval of sub-processors

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far this is possible.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice or immediately. In such situations, the data processor will notify the data controller of such change as soon as possible.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof before such change is to take effect. The data controller shall only object to such changes if the data controller has reasonable and specific grounds for such refusal.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed Services. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services, regardless if they cannot be provided to the data controller.

If it has been specifically agreed that the data processor cannot use sub-processors without the data controller's prior approval, the data controller accepts that this may mean that the data processor may be prevented from providing Services. If the data controller has refused any changes in terms of addition or replacement of sub-processors, non-provision of Services will not be considered a breach of the parties' Service Agreement that can be ascribed to the data processor in situations where not-performance may be ascribed to matters relating to a sub-processor.

Appendix C – Instruction pertaining to the use of personal data

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

The processing of personal data by the data processor on behalf of the data controller shall be carried out in accordance with the Service Agreement concluded between the data controller and the data processor.

The data processor bases its management system for information security on the principles in the ISO 27001 security framework and has implemented the relevant controls defined by this standard. In addition, the data processor has implemented a management system for secure processing of personal data.

These controls are managed in an ISMS system for ISO 27001, and a PIMS system for GDPR. Thereby, controls are documented on an ongoing basis, and findings from internal audits are used for ongoing improvements.

The data controller has instructed the data processor in processing data on the basis of the Services agreed and on the basis of the instructions below.

C.1.1 Consultancy Services

Data processing can only be based on specifically agreed consultancy projects.

C.2. Security of processing

The level of security shall reflect a generally high level of security reflecting the types of data being processed. Technical and organisational measures are implemented pursuant to the ISO 27001 standard, and checks from ISO 27002 are implemented and complied with.

In addition, the level of security shall reflect the specifically agreed services in the parties' Service Agreement.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the agreed level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

At the time of commencement, the obligation for the data processor to carry out security measures involves to implement and maintain the security level described in the document "Organisational and Technical Measures". The document is available at https://legal.itm8.com. These security requirements represent the data controller's total requirements in terms of security matters with the data processor based on the data controller's own risk assessment.

C.3 Assistance to the data controller

As far as possible – and within the scale and extent specified below – the data processor shall assist the data controller in accordance with Clause 9.1 and 9.2 by implementing the following technical and organisational measures:

At the specific request of the data controller, the data processor shall, as far as possible and taking into account the nature of the processing, assist the data controller with appropriate technical and organisational measures, in the fulfilment of the data controller's obligations to respond to requests for the exercise of the data subjects' rights pursuant to the General Data Protection Regulation.

If a data subject makes a request to the data processor to exercise its rights, the data processor shall notify 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 also, upon specific request, assist the data controller in ensuring compliance with the obligations of the data controller in relation to:

- Implementation of appropriate technical and organisational measures
- Security breaches
- Notification of a personal data breach to the data subject
- Conducting impact assessments
- Prior consultation of the supervisory authorities.

C.4 Storage period/erasure procedures

The data controller itself disposes personal data processed by the data processor on behalf of the data controller. Thus, personal data made available for the data processor's processing will be stored until erased by the data controller or until termination of the Services relating to processing of personal data.

Upon deletion of personal data in the data controller's systems, these personal data will be deleted in the data processor's backup system based on the agreed retention period (backup history) for each system.

At the request of the data controller, the data processor will assist with erasure or return of personal data as further instructed by the data controller.

C.5 Processing location

The processing of the personal data covered by the provisions cannot, without the prior written approval of the data controller, take place at locations other than the following:

Processing of personal data occurs at one or more of the following addresses

- The data processor's addresses
- Data centers used by the data processor

- Sub-processors, as well as their sub-processor addresses

In addition, remote work can be conducted in accordance with the data processor's remote work policy.

C.6 Instruction for transfer of personal data to third countries

The data controller has authorised and thereby instructed the data processor to transfer personal data to a third country as further specified below. In addition, by subsequent written notification or agreement the data controller can provide instructions or specific consent pertaining to the transfer of personal data to a third country.

If the data controller does not in the Clauses or subsequently provides documented instructions pretraining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.6.1 General approval of transfer of personal data to secure third countries

With these Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third country/the relevant area/the relevant sector has a sufficient level of protection.

For transfers to organisations in the United States that are certified under the EU-U.S. Data Privacy Framework ("DPF"), the Controller also provides by the Provisions its general and prior approval (instruction) for the Data Processor to make transfers of personal data to these organisations. The Data Processor is at any time obliged to ensure that the sub-processors used have the required certification.

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

The data controller instructs the data processor to use the following sub-processor(s) where transfers of personal data to third countries take place:

NAME	COMPANY NUMBER	DESCRIPTION OF PROCESSING	TRANSFER TO A THIRD COUNTRY

When entering into the Clauses, the data controller has given consent to the use of the above sub-processor(s) and instructed on the transfer of personal data to third countries for the provision of the Services.

If the European Commission's Standard Contractual Clauses ("SCC") for the transfer of personal data to a third country are used as the transfer basis, the data processor and/or any sub-processor shall be entitled to enter into such SCCs with the relevant sub-processor.

In the event that the European Commission produces new SCCs after the conclusion of the Service Agreement, the data processor is authorised to replace, update and apply the SCCs in force at any time.

The contents of this instruction and/or the Clauses shall not be deemed to modify the contents of the SCCs.

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

Pursuant to Articles 24 and 28 of the General Data Protection Regulation, the data controller is entitled and obliged to monitor the data processor's processing of personal data on behalf of the data controller. The data controller's monitoring of the data processor may consist in one of the following actions from the data controller:

- Self-checking based on documents provided to the data controller by the data processor;
- written inspection; or
- physical inspections.

C.7.1 Self-checks

Via the website **https://legal.itm8.com**, the data controller can access a range of documents for the purpose of self-checking, including:

- A description of organizational and technical controls with the data processor.
- Information security policy

C.7.2 Written inspection and physical inspection

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

In case of a request for a written or a physical inspection, the procedure below shall be applied.

Procedure and reporting of written inspection or physical inspection:

- The data controller sends an inspection form to the data processor by email to gdpr@improsec.com with a request for a written or a physical inspection.
- The data processor confirms receipt and confirms the date for such inspection.

- The inspection is made.
- The data controller shall forward any observations resulting from the inspection to gdpr@improsec.com.
- The data processor will review and provide any comments to the data controller's observations (can be repeated several times).
- The data controller shall carry out its final conclusion on the inspection and shall forward the report to the data processor.
- The inspection is ended.

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

Based on the data processor's risk assessment and having regard to the specific processing activities, the data processor will carry out audits, including inspections, of sub-processors' processing of personal data, either in the form of self-auditing of audit certificates and equivalent (where possible), written inspection or physical inspection, or a combination thereof.

If requested by the data controller, the data controller may obtain additional information about the control measures introduced and implemented towards each sub-processor.

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

D.1 In 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 shall prevail over any corresponding regulation in Service Agreements between the parties regarding the part of the activities and responsibilities of the data processor related to the data processing, while the performance of all other activities related to the provision of agreed Services shall be 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 performance 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 relating to the data processor's processing activities, Appendix D shall also prevail.

D.2 Consequences of the data controller's illegal instructions

The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller. Consequently, the data processor is not liable for any claims arising from the data processor's acts or omissions, to the extent such acts or omissions is a data processing activity exercised in accordance with the data controller's instructions.

D.3 Implementation of other security measures

The data processor is entitled to implement and maintain other security measures than what has been specified in the Service Agreement Appendix C.2, however, provided that such other security measures provide an overall level of security equivalent to the prescribed security measures.

D.4 Use of Third Party Services

Notwithstanding clause 7, it is agreed that if the Data Processor uses Standard Third Party Services, which means services that do not contribute specifically to the performance of a specific Service Agreement, but which are used by the Data Processor as supporting services to a plurality of customers, regardless of whether this may be integrated into the Services or made available to the Data Controller as a separate Service, for example, but not limited to services provided via a cloud provider and made available under its standard terms (*"***Standard Third Party Service"**), the Data Processor is not responsible for any processing activities of these Third Party Providers (as a sub-processor) in connection with the provision of these Standard Third Party Services.

The Third Party Provider's own terms for the processing activities as a sub-processor can be found on *https://legal.itm8.com* as it is the Data Controller's own responsibility to ensure that these terms satisfactorily meet requirements for the Third Party Provider's processing activities. The Data Controller has been made aware that these terms may be changed from time to time by the individual Third Party Provider, and the Data Controller must thus continuously ensure that these meet the requirements for the processing activities.

By the Provisions, the Data Controller gives its consent to and instructions that such specific processing activities take place on the Third Party Provider's terms.

D.5 Erasure and return of data

It has been agreed between the parties that the data controller will instruct the data processor on erasure and return of personal data in connection with termination of the Clauses.

At the latest thirty (30) days after the processing of personal data has terminated, the data controller will notify the data processor whether all personal data is to be erased or returned to the data controller. If personal data is to be returned to the data controller, the data processor shall also erase any copies. The data processor must ensure that any sub-processors will also comply with the notice from the data controller.

The obligation of erasure shall not apply with respect to (i) copies of electronically exchanged personal data stored as part of automated backup functions, provided that access thereto is limited to IT or compliance personnel and provided that all such data is still processed in accordance with the terms of these Clauses, and (ii) personal data that must be stored by the data processor pursuant to mandatory legislation.

If the data processor has not received information from the data controller within thirty (30) days after the processing of personal data has terminated, the data processor will send a reminder to the data controller. If the data controller does not 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 such personal data without any further notice.

The data processor is entitled to payment for the data processor's processing activities until the time when 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 – in general

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

Such payment is calculated on the basis of the time spent and the agreed hourly rates in the Service Agreement for the provision of Services, and if no hourly rates have been agreed, the data processor's current hourly rates will apply.

Any external costs incurred, including costs to be borne 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 security measures contained in a Service Agreement relating to the provision of Services or to Appendix C, the data processor will faithfully seek to meet such requirements to the extent technically feasible and compatible with meeting other requirements for the Services concerned.

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

D.6.3 Inspection and audit

The data processor is entitled to payment for the data controller's inspection and audit. Such payment is calculated on the basis of the time spent and the agreed hourly rates in the Service Agreement regarding supply of Services, and if no hourly rates have been agreed, the data processor's current hourly rates will be applied.

Any external costs incurred, including costs to be borne 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 will be regulated and processed in accordance with the parties' Service Agreement, as supplemented below:

a) In cases where the data processor has paid amounts to data subjects in accordance with Article 82 of the General Data Protection Regulation or Article 26 of the Danish Liability in Damages Act, the data processor shall have full recourse against the data controller for the amount paid which exceeds the agreed limitation of liability in the parties' Service Agreement for the provision of Services. The parties have hereby contractually derogated

from Article 82(5) of the General Data Protection Regulation and Article 26 of the Danish Liability in Damages Act.

b) Regardless of Article 82(5) of the General Data Protection Regulation, and if the data processor has paid damages to an injured party, and this amount does not correspond to damages in full, such data processor may have a claim for recourse pursuant to the principle in Article 82(5).

c) As regards other compensation for non-financial loss to data subjects, the principle in Article 82 furthermore applies as regards the internal final allocation of responsibility between the data processor and the data controller.

d) A party cannot make a claim for recourse or damages towards the other party for fines or other penalties awarded pursuant to Section 41 of the Danish Data Protection Act and for penalties accepted pursuant to Section 42 of the Danish Data Protection Act.

e) The data processor's total liability for breach of the Clauses shall be subject to any limitations on the amount (and shall be included in the maximum damages) that may be set out in the parties' Service Agreement. Liability (including such damages or other financial compensation as may be awarded to the data controller under the Service Agreement) shall be limited to an amount less than 150% of the amount received by the data processor in the twelve (12) months preceding the harmful act. If a period of twelve (12) months has not yet passed, the limitation of liability will be calculated as the average of the amounts received during the months passed multiplied by twelve (12).

f) The data processor's liability for breach of the Clauses shall not extend to indirect loss, including operating losses, consequential loss or other indirect loss.

g) The data processor shall not be liable for breach of the Clauses caused by computer viruses, cybercrime or other forms of unauthorised interference by third parties with the data controller's or the data processor's IT systems, unless the loss is directly related to the failure to meet the security requirements in the parties' Service Agreement.

D.8 Derogations

The parties have agreed on the following derogations from the Clauses and this Appendix:

PROVISIONS/CLAUSE	DEROGATIONS FROM THE PROVISIONS
Clause 7.6	The parties have agreed that clause 7.6 of the Clauses (as specified below) shall not apply between the parties. Thus, the following text shall be deleted from the Clauses: "*the data processor shall in its Service Agreement with the sub-processor include the data controller as a third-party beneficiary in the event of the bankruptcy of the data processor to enable the data controller to assume the data processor's rights and invoke these as regards the sub-processor, e.g. so that the data controller is able to instruct the sub-processor to perform the erasure or return of data*."

APPENDIX/CLAUSE	DEROGATIONS FROM THE APPENDICES
Reference	Derogation