itm8®

Itm8 | Improsec A/S

Appendix A-C under itm8 Group's Data Processing Agreement

Content

itm8 Group's Data Processing Agreement appendices A-C	2
Background	2
Appendix A – Information about the processing	3
Appendix B – Authorised Sub-processors	6
Appendix C – Instruction pertaining to the use of personal data	8

itm8 Group's Data Processing Agreement appendices A-C

Background

Pursuant to Article 28(3) of Regulation 2016/679 (General Data Protection Regulation) for the processing of personal data by the data processor, the Customer (hereinafter the "the data controller") and the Supplier (hereinafter "the data processor") have entered into itm8 Group's Data Processing Agreement (hereinafter the "Clauses"), which is attached to the applicable Cooperation Agreement (hereinafter the "Cooperation Agreement") between the parties.

The parties have entered into the Work Order of [date] for the provisions of [service] adopted with the Cooperation Agreement.

As a part of the delivery of the Services under the Work Order, the data processor process personal data on behalf of the data controller. In addition to the applicable Work Order and the adopted itm8 Group's Data Processing Agreement, the parties have adopted this **Appendices A-C.**

Appendices A-C is attached as an appendix to the applicable Work Order and contains the specific requirements in relation to e.g. the data controller's instruction, the subject matter of the processing, the nature of the processing, the use of sub-processors, security measures, etc.

Appendices A-C shall be considered an integral part of the Cooperation Agreement for the provisions of the Services specifies in the relevant Work Order. The adoption of Appendices A-C shall therefore be deemed to have occurred upon the conclusion of the applicable Work Order.

Appendices A-C shall be effective from the entry into force of the applicable Work Order and until its termination, unless the parties enter into a new Appendices A-C replacing this Appendices A-C.

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.