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 shall deliver the following services:

Selected (x)	Processing activities
☒	Hosting and operations Specified as Services in the categories Backup & Restore, Datacenter, Server Operation, Network and Workplace in the appendix "Leverandørens Services" to the parties' agreement regarding delivery of Services.
☒	Support
☒	Consultancy services
☒	Database administration
☒	Configuration and development
☒	Operation and servicing of application services
☒	Security services

A.1.1 Hosting and operations

If Hosting and operations has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is the delivery of hosting and operation of the data controller's IT systems, including backup, monitoring, maintenance and support, as further specified in the agreement regarding delivery of Services entered into between the parties. This also includes specific tasks ordered by the data controller.

A.1.2 Support

If support has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is the delivery of support services to the data controller, as further specified in the Service Agreement entered into between the parties. This also includes specific tasks ordered by the data controller.

A.1.3 Consultancy services

If consultancy services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is to perform specifically agreed consultancy tasks. The purpose will therefore vary, but will always be connected to an agreed consultancy task.

A.1.4 Database administration

If database administration has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is to perform administration tasks on the data controller's databases and database servers, including administration of tables, jobs, performance optimisation, backup, database storage, configuration and similar tasks, as further specified in the Service Agreement entered into between the parties. Specific tasks ordered by the data controller are also performed.

A.1.5 Configuration and development

If configuration and development has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is to perform specifically agreed development and configuration tasks on the data controller's IT systems and applications.

A.1.6 Operation and servicing of application services

If operation and servicing of application services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is the delivery of the application services agreed in the main agreement to the data controller. The delivery includes, for example, implementation, operation, development and support of the selected application services, as further specified in the Services Agreement entered into between the parties.

A.1.7 Security services

If security services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The purpose of the processing is the delivery of security services to the data controller. The delivery includes, for example, managed or unmanaged Security Information and Event Management (SIEM), penetration testing or incident management following a security breach.

A.2. The data processor's processing of personal data on behalf of the data controller primarily concerns (the nature of the processing)

A.2.1 Hosting and operations

If hosting and operations has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor provides hosting and operation of the data controller's IT systems. The primary purpose of the processing is therefore hosting, including storage of the data controller's personal data, and ongoing operation, including monitoring, backup and maintenance of the data controller's IT systems containing personal data.

In the specific cases, the processing may include, among other things, organisation, structuring, facilitation, temporary storage, filtering, troubleshooting, adaptation or alteration, retrieval, searching, use, alignment, combination, restriction or erasure of personal data where this is necessary in connection with the data processor's delivery of Services to the data controller, or where it is necessary in order to comply with a specific request from the data controller.

A.2.2 Support

If support has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor provides support to the data controller's employees, etc. All work that the data processor provides as part of the support and that involves processing of personal data on behalf of the data controller takes place at the data controller's specific request.

The data processor supports the data controller with the data controller's day-to-day operation of its IT systems. At the data controller's request, the data processor may take over the data controller's handling of the data controller's IT systems at their workplace or servers via TeamViewer or Remote Desktop for a specific task. In addition, the data processor may access systems in order to handle troubleshooting and operational tasks.

In the event of errors in software or in the data controller's IT systems in general, the data processor may retrieve a database from the data controller for the purpose of troubleshooting, corrections, etc. This only takes place following prior specific agreement.

In the specific cases, the processing may include, among other things, organisation, structuring, facilitation, temporary storage, filtering, troubleshooting, adaptation or alteration, retrieval, searching, use, alignment, combination, restriction or erasure of personal data where this is necessary in connection with the delivery of the agreed services, or where it is necessary in order to comply with a request from the data controller.

A.2.3 Consultancy services

If consultancy services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor performs tasks in connection with specific and delimited assignments. The consultancy tasks are performed on the data controller's systems and data, and the processing will be defined in the specific assignment.

The tasks are ordered and defined by the data controller, and the data processor participates to the extent necessary in ensuring a correct definition of the task.

A.2.4 Database administration

If database administration has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor provides administration of the data controller's databases and database servers. The primary purpose of the processing is therefore administration, optimisation, maintenance, monitoring and troubleshooting of the data controller's databases containing personal data.

The primary purpose of the processing is not to process personal data, but in connection with the performance of the data processor's obligations, processing of data may occur in the data controller's databases. This may include, among other things, organisation, temporary storage, filtering, troubleshooting, adaptation or alteration, retrieval, searching, combination or erasure of personal data where this is necessary in connection with the data processor's delivery of Services to the data controller, or where it is necessary in order to comply with a specific request from the data controller.

A.2.5 Configuration and development

If configuration and development has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor performs tasks related to the development and configuration of the data controller's business applications. This includes the development of components for ERP systems, CRM, SharePoint and other applications. The tasks are performed by specific agreement with the data controller.

A.2.6 Operation and servicing of the following application services

If operation and servicing of the following application services has been selected as a service in the table in Appendix A.1., the following applies:

The data processor provides maintenance, configuration, updates, development, support, hosting and operation of the selected application services to the data controller, as further specified in the Services Agreement entered into between the parties.

A.2.7 Security services

If security services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor performs monitoring, configuration, reporting, penetration testing and incident management following security breaches, as further specified in the Services Agreement entered into between the parties.

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

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

☒ Name

☒ Address

☒ E-mail

☒ Telephone number

☒ Financial information

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

☒ Racial or ethnic origin.

☒ Political opinions.

☒ Religious beliefs.

☒ Philosophical beliefs.

☒ Trade union membership.

☒ Health data, including abuse of medicine, drugs, alcohol, etc.

☒ Sex life.

Information about purely private matters of individuals (cf. section 8 of the Danish Data Protection Act):

☒ Criminal offences.

☒ Significant social problems.

Other purely private matters not mentioned above:

☒ Other private matters.

Information about CPR number (Danish civil registration number) (cf. section 11 of the Danish Data Protection Act):

☒ CPR numbers.

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

Categories of data subjects, identified or identifiable natural persons, to whom the data processor's processing activities relate:

☒ Employees

☒ Children

☒ The data controller's own customers

A.5. The data processor's processing of personal data on behalf of the data controller may begin after these Clauses have entered into force. The processing has the following duration:

The data processor's processing of personal data on behalf of the data controller begins after the parties' agreement regarding delivery of Services enters into force, and continues until that agreement terminates.

Appendix B – Sub-processors

B.1. Approved sub-processors

The sub-processors used from time to time appear in the data processor's applicable list of sub-processors, which is available on the data processor's Legal landing page https://legal.itm8.com. The list constitutes the complete and updated list of the sub-processors that the data controller has approved under these Clauses. The data processor is entitled to add, replace and remove sub-processors on an ongoing basis, provided that the data controller is informed in accordance with the Clauses of the data processing agreement

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

B.2. Notice period for the approval of sub-processors

The data processor's notification of any planned changes regarding the addition or replacement of sub-processors must reach the data controller no later than 30 days before the use or the change is to take effect, in so far as this is readily possible.

Notwithstanding the above, the data controller accepts that there may be special cases in which a specific need may arise for the change regarding the addition or replacement of sub-processors to take place at shorter notice or with immediate effect. In such cases, the data processor will notify the data controller of the change as soon as possible. Special cases may include, but are not limited to, the following situations:

- Where the sub-processor is unable to deliver the agreed service due to its bankruptcy, or
- Cases where the sub-processor is in breach of the contract, or
- Where changes in law or practice immediately prevent the use of the sub-processor in question.

If the data controller objects to the changes, the data controller must notify the data processor thereof before the notified effective date of the change. The data controller may only object if the data controller has reasonable, specific grounds for doing so.

In the event of an objection by the data controller, the data controller simultaneously accepts that the data processor may be prevented from delivering all or part of the agreed services. Such non-performance cannot be attributed to a breach by the data processor. The data processor retains its claim for payment for such services, irrespective of the fact that they cannot be delivered to the data controller.

Where it has been 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 the Services. If the data controller has refused changes regarding the addition or replacement of sub-processors, a failure to deliver services will therefore not be regarded as a breach of the parties' agreement regarding delivery of Services attributable to the data processor in cases where the non-performance can be attributed to circumstances relating to a sub-processor.

Appendix C - Instructions concerning the processing of personal data

C.1. The subject of the processing/instructions

The data processor's processing of personal data on behalf of the data controller takes place in accordance with the Service Agreements entered into between the data controller and the data processor.

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

The controls are managed in an ISMS system for ISO 27001 and a PIMS system for GDPR. Controls are thereby documented on an ongoing basis, and findings from internal audits are used for continuous improvement.

In addition, the data processor is audited once a year, resulting in an ISAE 3402 report for operations, hosting and support, as well as an ISAE 3000 report. The data processor also maintains an ongoing ISO 27001:2022 certification.

The latest reports and certificate are always available here: Legal & Compliance in itm8.

The data controller has instructed the data processor to process data on the basis of the Services agreed upon and on the basis of the instructions set out below.

C.1.1 Hosting and operations

If hosting and operations has been selected as a processing activity in the table in Appendix A.1., the following applies:

Storage and backup as well as the associated processing activities that are necessary in connection with the delivery of the agreed services, or that are necessary in order to comply with a request or instruction from the data controller. The processing operations carried out by the data processor includes:

- Backup and backup controls.
- Patch Management.
- Operation and maintenance of systems and infrastructure.
- Virus scanning and follow-up on virus alerts.
- Installations and configurations.
- Handling of monitoring alerts.
- Documentation of assets, procedures and controls.

C.1.2 Support

If support has been selected as a processing activity in the table in Appendix A.1., the following applies:

Processing of data is carried out in accordance with the services associated with the support services contained in the parties' agreement regarding delivery of Services, or specific cases initiated by the data controller.

C.1.3 Consultancy services

If Consultancy services has been selected as a processing activity in the table in Appendix A.1., the following applies:

Processing of data may be carried out solely on the basis of specifically agreed consultancy tasks.

C.1.4 Database administration

If database administration has been selected as a processing activity in the table in Appendix A.1., the following applies:

Processing of data is carried out in accordance with the services associated with the database administration services contained in the parties' agreement regarding delivery of Services, or specific cases initiated by the data controller.

C.1.5 Configuration and development

If configuration and development has been selected as a processing activity in the table in Appendix A.1., the following applies:

Processing of data is carried out in accordance with the tasks agreed with the data controller.

C.1.6 Operation and servicing of the following application services

If operation and servicing of the following application services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor's processing of personal data on behalf of the data controller takes place as part of the delivery of the selected application services to the data controller, as further specified in the Services Agreement entered into between the parties, including:

- Backup.
- Support.
- Hosting.
- Operation and maintenance.
- Configuration.
- Updates.
- Documentation.

And associated processing activities that are necessary in connection with the delivery of Services, or that are necessary in order to comply with a request or instruction from the data controller.

C.1.7 Security services

If security services has been selected as a processing activity in the table in Appendix A.1., the following applies:

The data processor's processing of personal data on behalf of the data controller takes place as part of the delivery of the selected security services to the data controller, as further specified in the Services Agreement entered into between the parties, including:

- Monitoring.
- Configuration.
- Reporting.
- Maintenance.
- Documentation.

C.2. Security of processing

The level of security must reflect a generally high level of security that reflects the types of data being processed. Technical and organisational measures have been implemented on the basis of the ISO 27001 standard, and relevant controls from Annex A have been implemented.

In addition, the level of security must reflect the specific services agreed in the parties' agreement regarding delivery of Services. The data processor is thereafter entitled and obliged to make decisions as to which technical and organisational security measures are to be implemented in order to establish the agreed level of security.

However, the data processor must – in any event and as a minimum – implement the following measures, which have been agreed with the data controller:

At the time of entering into the agreement, the data processor's obligation to implement security measures means that the data processor must implement and maintain the level of security described in the document "Organisational and technical measures". The document is available at Legal & compliance in itm8. These security requirements constitute the data controller's overall requirements for security conditions at the data processor, based on the data controller's own risk assessment.

C.3 Assistance to the data controller

The data processor must, as far 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 data controller's specific request, the data processor assists, taking into account the nature of the processing and as far as possible, the data controller by means of appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for exercising the data subjects' rights as laid down in the General Data Protection Regulation.

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

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

- Implementation of appropriate technical and organisational measures.
- Security breaches.
- Communication of a personal data breach to the data subject.
- Carrying out data protection impact assessments.
- Prior consultations with the supervisory authorities.

C.4 Storage period/erasure routine

The data controller itself has control over the personal data that the data processor processes on behalf of the data controller. The personal data entrusted to the data processor's processing is therefore stored until the data controller itself erases the data or until the cessation of the Services concerning the processing of personal data.

Upon erasure of personal data in the data controller's systems, such personal data will be erased in the data processor's backup system in accordance with the agreed storage period (backup history) for each individual system.

At the data controller's request, the data processor assists with the erasure or return of personal data as further instructed by the data controller.

C.5 Location of processing

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

- The data processor's addresses.
- Data centres used by the data processor.
- Sub-processors and the addresses of their sub-processors.

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

C.6 Instructions concerning the 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, the data controller may, by a subsequent written notice or agreement, provide an instruction or specific approval concerning the transfer of personal data to a third country.

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

C.6.1 General approval concerning the transfer of personal data to safe third countries

By these Clauses, the data controller gives its general and prior approval (instruction) for the data processor to transfer personal data to third countries where the Commission has determined that the third country/the relevant territory/the relevant sector ensures an adequate level of protection.

For transfers to organisations in the USA that are certified under the EU-U.S. Data Privacy Framework ("DPF"), the data controller also gives, by these Clauses, its general and prior approval (instruction) for the data processor to transfer personal data to such organisations. The data processor is obliged at all times to ensure that the sub-processors used hold the required certification.

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

The data controller instructs the data processor to use the sub-processors that appear from time to time on the list below, including sub-processors that transfer personal data to third countries: https://legal.itm8.com/Default.aspx?ID=12265&Purge=True

By entering into the Clauses, the data controller has approved the use of the sub-processors appearing on the above list and has instructed the data processor to transfer personal data to third countries to the extent necessary for the delivery of the Services.

If the EU 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 is entitled to enter into such SCCs with the relevant sub-processor.

In the event that the EU Commission prepares new SCCs after the conclusion of the agreement, the data processor is authorised to replace, update and apply the SCCs in force from time to time.

The content of these instructions and/or the Clauses is not considered to change the content of the SCC.

C.7 Procedures for the data controller's audits, including inspections, of the processing of personal data entrusted to the data processor

Pursuant to Articles 24 and 28 of the General Data Protection Regulation, the data controller has the right and the duty to carry out audits of the data processor's processing of personal data on behalf of the data controller. The data controller's performance of audits of the data processor may take place by the data controller carrying out one of the following actions:

- self-assessment on the basis of documents that the data processor makes available to the data controller.
- written inspection, or
- physical inspections.

C.7.1 Self-assessment

The data controller has access at Legal & Compliance in itm8 to a number of documents for use in carrying out self-assessment, including:

- The latest version of the data processor's ISAE 3402 report (published every year).
- The latest version of the data processor's ISAE 3000 report (published every year).
- The latest version of the ISO 27001 certificate.
- Description of organisational and technical measures at the data processor.
- Information security policy.

C.7.2 Written audit and physical inspection

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

When requesting the performance of a written audit or physical inspection, the procedure set out below is used.

Procedure and reporting for a written audit or physical inspection:

- The data controller sends their audit questionnaire to the data processor by e-mail to gdpr@itm8.com requesting the performance of an audit and/or inspection.

- The data processor confirms receipt and states the final date for the performance of the audit and/or inspection.
- The performance of the audit and/or inspection takes place.
- The data controller sends any observations from the audit to gdpr@itm8.com.
- The data processor reviews and comments on any observations of the data controller (this may be repeated several times).
- The data controller draws up its final conclusion on the audit and sends the report to the data processor.
- The audit is concluded.

C.8 Procedures for audits, including inspections, of the processing of personal data entrusted to sub-processors

On the basis of the data processor's risk assessment and taking into account the specific processing activities, the data processor carries out audits, including inspections, of sub-processors' processing of personal data either in the form of self-assessment of audit reports and the like (where possible), written audit or physical inspection, or a combination thereof.

At the data controller's request, the data controller may obtain further information about which control measures have been initiated and carried out in respect of the individual sub-processors.

Appendix D – The parties' regulation of other matters

D.1 General

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

The clauses of this agreement take precedence over any corresponding regulation in Service Agreements between the parties regarding that part of the data processor's activities and responsibilities that relate to the processing of data, whereas the performance of all other activities concerning the delivery of agreed Services is governed by 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 discrepancy between the Clauses and the terms set out in this Appendix D, Appendix D shall take precedence, and if the Service Agreement otherwise contains terms concerning the data processor's processing activities, Appendix D shall likewise take precedence.

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

The data controller is aware that the data processor depends on the data controller's instructions to the extent to which the data processor is entitled 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 such acts or omissions constitute a 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 compared with those set out in the agreement regarding delivery of Services and Appendix C.2, 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 that are identified in a Service Agreement as suppliers of Standard Third-Party Services, any processing activities of the Third-Party Suppliers (as sub-processor) in connection with the delivery of such Standard Third-Party Services will be governed by the Third-Party Supplier's own terms for the processing activities as sub-processor.

The data processor has made the terms available at https://legal.itm8.com, and it is the data controller's own responsibility to familiarise itself with these and otherwise to ensure that these terms satisfactorily meet the requirements for the Third-Party Supplier's processing activities.

The data controller has been made aware that these terms may be changed on an ongoing basis by the individual Third-Party Supplier, and the data controller must therefore continuously ensure that they meet the requirements for the processing activities.

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

By accepting the Clauses, the data controller simultaneously gives its acceptance of, and instruction for, processing activities to take place on the Third-Party Supplier's terms.

D.5 Erasure and return of data

It is agreed between the parties that the data controller instructs on the data processor's erasure and return of personal data in connection with the termination of the Clauses.

No later than 30 days after the processing of personal data has ceased, the data controller must notify the data processor whether all personal data is to 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 erase any copies. The data processor must ensure that any sub-processors likewise comply with the notice from the data controller.

The erasure obligation does not cover (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 such data continues to be processed in accordance with the Clauses, and (ii) personal data that must be retained by the data processor pursuant to mandatory legislation.

If the data processor has not received notice from the data controller within 30 days after the processing of personal data has ceased, the data processor sends a reminder to the data controller. If the data controller subsequently fails to 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 the personal data without further notice.

The data processor is entitled to payment for its processing activities up until the point in time at which 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 remuneration for such Services, has undertaken to perform the Clauses, the data processor will be entitled to remuneration for assistance in accordance with the assistance services agreed in the Clauses, including clause 9.

The remuneration is calculated on the basis of the time spent and the hourly rates agreed in the Service Agreement regarding delivery of Services and, where no hourly rates have been agreed therein, in accordance with the data processor's applicable hourly rates.

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

D.6.2 Implementation of other security measures

If the data controller's instructions, etc., as well as the data processor's ongoing assessments in general, result in stricter requirements than the requirements for security measures contained in a Service Agreement concerning the delivery of Services or in Appendix C, the data processor will loyally seek to accommodate such requirements provided that this is technically possible and compatible with meeting the other requirements for the Services concerned.

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

D.6.3 Audits and inspections

The data processor is entitled to remuneration for the data controller's performance of audits and inspections. The remuneration is calculated on the basis of the time spent and the hourly rates agreed in the Service Agreement regarding delivery of Services and, where no hourly rates have been agreed therein, in accordance with the data processor's applicable hourly rates.

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

D.7 Liability and breach

Any breach of the Clauses is governed and handled in accordance with the parties' Service Agreement regarding delivery of Services, with the following additions;

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 – Separate national data protection requirements

If the data controller is located outside Denmark, separate requirements apply which are in accordance with national data protection rules in the data controller's home country. The national special rules can be found here: https://legal.itm8.com/Default.aspx?ID=12295&Purge=True