DATA PROCESSING AGREEMENT

(Last Updated: 19th June 2026)

Table of Contents

1. PREAMBLE

1. These Clauses (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 regarding 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 provision of the agreed services of the main agreement, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

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

6. 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.

7. 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.

8. 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.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. Appendix E contains any deviations from the standard Clauses.

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

12. 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 legislation.

2. 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 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.

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. Data minimization and limiting exposure of sensitive data Prior to granting the Data Processor access to any systems or personal data, the Data Controller shall ensure that only personal data strictly necessary for the defined purposes is provided or made accessible, in accordance with the principles of data minimization and purpose limitation.

5. Instructions, authorization, and scope of processing:

    a. The Data Controller's documented instructions and authorization under the Agreement extend to the personal data of its data subjects that the Data Controller provides or makes accessible to the Data Processor for the agreed purposes, only to the extent necessary for performance of the contracted services.

    b. It is the Data Controller's obligation to establish and maintain an appropriate legal basis for each processing activity (including, where applicable, valid consent meeting GDPR standards) and to provide all required transparency notices to data subjects.

6. Data subject requests and denial to execute data handling requests

    a. The Data Controller is solely responsible for assessing and responding to requests from data subjects under Chapter III GDPR. Considering the nature of the processing, the Data Processor shall assist the Data Controller insofar as possible and shall act only on the Data Controller's documented instructions.

    b. The Data Processor may decline to act on a data subject request made directly to it and will direct the requestor to the Data Controller unless the Data Controller has provided documented instructions to the contrary. The Data Processor may also decline to execute a Data Controller instruction where: (i) identity verification prerequisites set by the Data Controller have not been met; (ii) the request is outside the scope defined in the Agreement and documented instructions; (iii) the instruction, in the Data Processor's opinion, infringes applicable data protection law (in which case the Data Processor shall promptly inform the Data Controller); or (iv) execution is technically infeasible without additional agreed measures. In such cases, the Data Processor will notify the Data Controller without undue delay.

7. The Data Controller shall provision and maintain access for the Data Processor on a least-privilege, need-to-know basis and ensure prompt modification or revocation where access is no longer required for the agreed purposes.

8. The Data Controller warrants and represents that all required information has been or will be provided to data subjects in accordance with Articles 13 and 14 GDPR and that the Data Controller's authorization and instructions to the Data Processor are effective for all data subjects whose personal data the Data Controller provides or makes accessible for the agreed purposes, subject to the Controller's compliance with the preceding clauses.

3. 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, controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

3. Where, in the Data Processor's opinion, an instruction infringes applicable data protection law, falls outside the Agreement's scope, lacks required identity verification, or is technically infeasible without additional agreed measures, the Data Processor may decline to execute the instruction and shall promptly notify the Data Controller to obtain lawful, scoped, and feasible instructions.

4. Reliance on Controller authorization. The Data Processor is entitled to rely on the Data Controller's warranty that all instructed processing has an appropriate legal basis and required transparency, and that the Data Controller's authorization and instructions are effective for all data subjects whose personal data the Data Controller provides or makes accessible for the agreed purposes. The Data Processor is not obliged to verify the legal basis, but will promptly inform the Data Controller if, in the Data Processor's opinion, an instruction infringes applicable data protection law.

5. The Data Processor shall not commence processing for any new purpose until it has received updated documented instructions confirming that the Data Controller has established the applicable legal basis and provided the required transparency.

6. The Data Processor may decline to act on requests received directly and will direct the requester to the Data Controller, unless otherwise instructed in writing by the Data Controller.

4. 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. Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor's authority are subject to the abovementioned confidentiality.

5. SECURITY OF PROCESSING

1. Article 32 GDPR stipulates that, considering 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;

2. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    a. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3. 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.

4. 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.

6. USE OF SUBPROCESSORS

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 material subprocessors at least ninety (90) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned material subprocessor(s). If the Customer objects to the appointment of a new material subprocessor on reasonable grounds regarding data protection and the parties cannot resolve such objection within a reasonable period, the Customer may terminate the affected Services by providing written notice to the Processor.

4. Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Data Controller can be found in Appendix B.

5. 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.

6. 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.

7. 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.

8. 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.

7. 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 organisation;

    b. Transfer the processing of personal data to a material subprocessor 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.

8. 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;

2. Notification obligation regarding rectification or erasure of personal data or restriction of processing.

    a. the right to data portability;

    b. the right to object;

    c. the right not to be subject to a decision based solely on automated processing, including profiling.

3. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.3., the Data Processor shall furthermore, considering 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, the Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

4. the Data Controller's obligation to without undue delay communicates 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;

    a. 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);

5. the Data Controller's obligation to consult the competent supervisory authority, the 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.

6. 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.

7. The Data Processor will assist the Data Controller in handling data subject requests and will not act independently on such requests unless instructed; if assistance would require actions beyond documented instructions or legal scope, the Data Processor may pause execution and seek clarification from the Data Controller.

9. 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:

4. 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;

5. the likely consequences of the personal data breach;

6. 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.

7. 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.

10. ERASURE AND RETURN OF DATA

1. The Processor shall comply with any retention periods or deletion instructions expressly set out in the applicable customer contract. In the absence of such retention periods or deletion instructions, the Processor shall, unless Union or Member State law requires storage of the Personal Data, without undue delay delete or return the Personal Data in accordance with applicable Data Protection Law.

2. The Data Processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

11. 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.6. and C.7.

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.

12. The parties' agreement on other terms

1. The parties agree that any 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.

2. The Processor shall not engage directly with data subjects regarding complaints or regulatory challenges and shall promptly refer any such communications to the Data Controller. For the avoidance of doubt, this clause governs the allocation of responsibilities between the parties and does not restrict any data subject's rights to lodge a complaint with a supervisory authority or seek judicial remedy under applicable law.

13. 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 10.1. and Appendix C.3., the Clauses may be terminated by written notice by either party.

On behalf of Data Processor,	***On behalf of the Data Controller,***
Date:	**Date:**
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**

14. Data controller and processor contacts/contact points

1. Each party shall designate a person responsible for the execution of the contract.
2. The parties may contact each other using the following contacts/contact points:
3. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

On behalf of Data Processor,	***On behalf of the Data Controller,***
Date:	**Date:**
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**

14. Change Notifications to the Data Controller

1. The Processor shall notify the Controller in writing of any material change affecting the processing, including: (a) scope/nature/purpose; (b) data transfer mechanisms or destinations; (c) retention/deletion policies; (d) data handling or security practices; (e) liability/indemnity terms. Material subprocessors changes are subject to chapter 6.3 and Appendix B.3.

2. Provide at least 90 days' prior notice where feasible; if not feasible due to urgency, notify without undue delay after implementation with justification. Notices shall include description, rationale, effective date, impact, safeguards, and any required actions.

3. If the Controller objects to the changes on reasonable grounds regarding data protection and the parties cannot resolve such objection within a reasonable period, the Customer may terminate the affected Services by providing written notice to the Processor.

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 IS:

A.1.1 SOC SERVICES

To provide security monitoring, detection, triage, investigation, and response services for the Data Controller, including identifying suspicious activity, indicators of compromise, compromised information, and other evidence relevant to security incidents affecting the Data Controller's environment.

A.1.2 INCIDENT RESPONSE SERVICES

To investigate, contain, analyze, and support the remediation of suspected or actual security incidents affecting the Data Controller, including identifying intruder activity, indicators of compromise, the scope and impact of the incident, and relevant remediation and recovery actions.

A.1.3 OFFSEC CONSULTANCY SERVICES

To perform offensive security consultancy and security assessment activities for the Data Controller in order to identify vulnerabilities, determine whether systems or data can be accessed, assess security posture and resilience, and support remediation planning.

A.1.4 THREAT INTELLIGENCE SERVICES

To provide and support the use of threat intelligence services for the Data Controller, including the hosting, collection, analysis, storage, correlation, and delivery of relevant threat intelligence and related service data, solely to provide the agreed services.

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 SOC SERVICES

The processing consists of collecting, storing, reviewing, correlating, and analyzing alert data, telemetry, logs, leak data, and forensic material, using both automated and manual investigation methods, in order to detect, investigate, and respond to suspicious or malicious activity. Because the content of alerts, leaks, and forensic material is not known in advance, personal data and potentially sensitive data may become available during the course of the service.

A.2.2 INCIDENT RESPONSE SERVICES

The processing consists of manual and automated investigation of systems, devices, accounts, network data, forensic images, logs, and collected artifacts in scope in order to identify attacker activity, indicators of compromise, root cause, affected assets, and incident impact. Depending on the scope of the incident, any personal data present in the compromised or affected systems, devices, or artifacts may be accessed, reviewed, extracted, correlated, analyzed, and used to support containment, eradication, recovery, and post-incident investigation.

A.2.3 OFFSEC CONSULTANCY SERVICES

The processing consists of manual and automated security testing, security assessment, and review of systems, devices, accounts, applications, and network data in scope. This may include accessing, reviewing, extracting, correlating, and analyzing data in order to identify vulnerabilities, security weaknesses, misconfigurations, or

paths to unauthorized access. The objective is to assess whether data or systems can be accessed and to document findings for remediation, rather than to use the data for any other purpose.

A.2.4 Threat Intelligence Services

The processing consists of any operation or set of operations performed on personal data as part of delivering the services, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The processing also includes hosting personal data and making relevant service outputs available to the Data Controller during the term of the services.

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

A.3.1 SOC Services

The types of personal data depend on the alerts, telemetry, leaks, or forensic material generated from the Data Controller's environment. Regular categories may include IP addresses, names, email addresses, usernames, domain names, computer names, browsing history, device metadata, and, where relevant, bank account numbers or other data present in leaks or forensic evidence. Personal data and potentially sensitive data may be included where they appear in the relevant source material.

A.3.2 Incident Response Services

The types of personal data depend on the scope of the incident and may include any personal data present in the compromised or affected systems, devices, accounts, logs, or artifacts. This may include, by way of example, IP addresses, names, email addresses, usernames, domain names, computer names, browsing history, bank account numbers, device and system metadata, and any other personal data encountered during investigation. Personal data and potentially sensitive data may be included where they appear in forensic material or other collected evidence.

A.3.3 OffSec Consultancy Services

The types of personal data depend on the systems and scope of the engagement and may include any personal data accessible in the in-scope systems, devices, applications, or accounts. This may include, by way of example, IP addresses, names, email addresses, usernames, domain names, computer names, browsing history, device and system metadata, and other personal data encountered during testing or assessment.

A.3.4 Threat Intelligence Services

The processing may include the following personal data:

- first name
- last name
- username
- email address
- IP address

Where relevant to the service, the processing may also include personal data relating to cyber threat actors, such as:

- IP address

- email address
- other relevant information uploaded to, or stored in, the service by the Data Controller

Sensitive data is not expected to be processed as part of this service, but cannot be categorically excluded if the Data Controller uploads such data or if it appears in service-related content.

A.4. Processing includes the following categories of data subject:

A.4.1 SOC Services

The categories of data subjects may include:

- employees of the Data Controller
- users of the Data Controller's systems and environments
- customers or customer representatives of the Data Controller
- other individuals whose personal data appears in alerts, logs, telemetry, leak data, or forensic material processed as part of the service

A.4.2 Incident Response Services

The categories of data subjects depend on the scope of the incident and may include:

- employees of the Data Controller
- users of the Data Controller's systems and environments
- customers or customer representatives of the Data Controller
- consultants, contractors, or other personnel represented in the affected systems
- any other individuals whose personal data is present in compromised or affected systems, devices, accounts, logs, or artifacts in scope

A.4.3 OffSec Consultancy Services

The categories of data subjects depend on the systems and scope of the engagement and may include:

- employees of the Data Controller
- users of the Data Controller's systems
- customers or customer representatives of the Data Controller
- consultants, contractors, or other personnel represented in the Data Controller's systems
- any other individuals whose personal data is present in the systems, devices, applications, or accounts in scope

A.4.4 Threat Intelligence Services

The categories of data subjects may include:

- employees
- agents

- consultants
- officers
- subcontractors
- outsourcers
- other representatives of the Data Controller
- cyber threat actors, where their personal data is relevant to the service and included in the information processed

A.5. THE SUBJECT OF / INSTRUCTION FOR THE PROCESSING

A.5.1 SOC SERVICES

The Data Processor is instructed to process personal data strictly as necessary to provide the agreed SOC services, including the collection, storage, correlation, review, and analysis of alerts, telemetry, logs, leak data, and forensic material, using manual and automated methods, in order to identify suspicious activity, indicators of compromise, intruder activity, and other information relevant to detection and response.

A.5.2 INCIDENT RESPONSE SERVICES

The Data Processor is instructed to process personal data strictly as necessary to provide the agreed incident response services, including investigating, collecting, preserving, reviewing, extracting, correlating, and analyzing relevant systems, logs, forensic material, and other artifacts in order to identify the nature, cause, scope, and impact of the incident and to support containment, eradication, remediation, recovery, and post-incident investigation.

A.5.3 OFFSEC CONSULTANCY SERVICES

The Data Processor is instructed to process personal data strictly as necessary to perform the agreed offensive security consultancy services, including testing, assessment, and analysis of in-scope systems, devices, applications, accounts, and artifacts, in order to identify vulnerabilities, security weaknesses, and potential unauthorized access paths and to support remediation planning.

A.5.4 THREAT INTELLIGENCE SERVICES

The Data Processor is instructed to process personal data strictly as necessary to provide the agreed threat intelligence services, including hosting, collecting, recording, storing, retrieving, analyzing, correlating, transmitting, and otherwise making available relevant service data and outputs to the Data Controller for the provision and use of the services only.

A.6. THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER MAY BE PERFORMED WHEN THE CLAUSES COMMENCE. PROCESSING HAS THE FOLLOWING DURATION:

Processing of personal data on behalf of the Data Controller shall not be time-limited and shall be performed until this Data Processing Agreement is terminated or cancelled by one of the Parties.

APPENDIX B: AUTHORIZED SUBPROCESSORS

B.1. APPROVED SUBPROCESSORS

On commencement of the Clauses, the Data Controller authorises the engagement of the following material sub-processors:

Name	Amazon Web Services - Dansk filial of Amazon Web Services EMEA SARL, Luxembourg	Google Cloud - Google Cloud EMEA Limited
VAT no.	DK39009323	IE3668997OH
CVR	39009323	
CRN	FC034225	660412
Address	c/o Spaces Ny Carlsberg Vej 80 Copenhagen V, 1799, Denmark	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland
Description	Backup	Operational systems, databases, data processing, and backups
Location(s) of processing	Frankfurt, Germany	Eemshaven, Netherlands Frankfurt, Germany

The Data Controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. THREAT INTELLIGENCE SERVICES (SECURITY ALLIANCE LTD.)

Where Threat Intelligence Services are utilized, such services are provided by the Data Processor's subsidiary, Security Alliance Limited. The Data Controller authorizes the subprocessors used by Security Alliance Limited for the provision of ThreatMatch Threat Intelligence Services, as listed below.

Name	Digital Ocean, LLC	Microsoft Ireland Operations Ltd	Amazon Web Services EMEA SARL	Google Cloud - Google Cloud EMEA Limited
VAT no.	NL854116552B01	IE8256796U	39009323	IE3668997OH
EIN/CRN	FC034225	256796	FC034225	660412
Address	101 Avenue of the Americas 10th Floor New	One Microsoft Place, South County Business	38 Avenue John F. Kennedy L-1855 Luxembourg	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland

	York, NY 10013 United States	Park, Dublin, D18 P521, Ireland		
Description	Operational systems, databases and data processing	AI Model inference	Backup	Operational systems, databases, data processing, and backups
Location(s) of processing	Frankfurt, Germany Amsterdam, Netherlands	Gävle, Sweden	Frankfurt, Germany	Eemshaven, Netherlands Frankfurt, Germany

B.3. Prior notice for the authorization of material sub-processors

The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of material subprocessors at least ninety (90) days in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned material subprocessor(s).

If the Customer objects to the appointment of a new material subprocessor on reasonable grounds regarding data protection and the parties cannot resolve such objection within a reasonable period, the Customer may terminate the affected Services by providing written notice to the Processor.

APPENDIX C: INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

C.1. SECURITY OF PROCESSING

The level of security shall consider:

The Data Processor has implemented the following measures:

- Data in transit is securely transmitted using TLS and any underlying block storage is encrypted. Data is under strict access control at all times.
- Data Access and Audit Logging is setup to detect abnormalities.
- Backups are access controlled and setup to maximise availability.
  Security incident management includes plans for timely restoration of services and personal data and with linkage to overall business continuity management.
- Access is provided to Data Controller through an online portal and can be protected by two factor authentication mechanisms.
- Remote working is allowed but through Data Processor agreed equipment applied with both storage and transport encryption.
- Only a small subset of Data Processors employees has access to the processed data and only selected employees have access to the raw data.
- Centralised log monitoring and alerting is performed.

C.2. ASSISTANCE TO THE DATA CONTROLLER

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Please refer to Clause C.1.

C.3. STORAGE PERIOD/ERASURE PROCEDURES

Personal data is stored for as long as the Clauses are effective after which the personal data is automatically erased by the Data Processor pursuant to Clause 10.

Upon termination of the provision of personal data processing services, the Data Processor shall return the personal data in accordance with Clause 10.1 unless the Data Controller – after the signature of the contract – has modified the Data Controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.4. PROCESSING LOCATION

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

- CSIS Security Group (Denmark)
- AWS Europe (Frankfurt, Germany)

- GCP Europe (Belgium, Finland, Ireland, Netherlands)
- The locations of processing used by the authorized sub-processors listed in Appendix B, as applicable to the relevant Service.

C.5. Instruction on the transfer of personal data to third countries

The Data Processor shall not, under this Agreement, transfer Personal Data to a third country unless it has obtained the Data Controller's prior written approval. For the avoidance of doubt, any support provided by AWS or GCP shall be limited to infrastructure-related and technical issues only and shall not include access to, use of, or any other processing of Personal Data.

C.6. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Controller can, at its own expense, obtain an audit from an independent third party concerning the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that either of the following types of reports may be used in compliance with the Clauses:

- ISAE 3000; or
- SOC 2 compliance certificate with appropriate Privacy Controls

The report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. The Data Controller will pay all expenses related to such request(s).

Based on the results of such an audit/inspection, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The Data Processor is not obligated to implement the suggested measures.

C.7. Procedures for audits, including inspections, of the processing of personal data being performed by subprocessors

The Data Processor commits to obtaining a report concerning the sub- processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. This is part of CSIS standard vetting procedures of subprocessors. Currently the following is requested:

ISO27001 compliance
SOC 2 compliance (ISAE3000)

If the data controller requests this, the reports shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. The Data Processor shall reasonably cooperate with the Data Controller in relation to any such request and shall use all reasonable efforts to support and facilitate the conduct of any new audit or inspection. For the avoidance of doubt, the Data Controller shall only bear all reasonable costs related to inspections of subprocessors where such inspections have been explicitly requested by the Data Controller.

The Data Processor is not obligated to implement the suggested measures. The Data Processor or the Data Processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing (when possible, e.g. AWS and GCP excluded due to security concerns). Such an inspection shall be performed, when the Data Processor (or the Data Controller) deems it required. The Data Controller will pay all expenses related to such subprocessor inspections.

Documentation for such inspections shall without delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

APPENDIX D: THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

Regardless of the regulation of the Data Controller and the Data Processor's liability in the General terms of Business, the liability of each of the Data Controller and Data Processor may not exceed an amount equal to the annual fee in Danish kroner. When calculating the total maximum liability of either the Data Controller or the Data processor under these Clauses, any liability under the General terms of Business shall be included.

Compensation for indirect losses and consequential damages, including but not limited to operating losses, loss of profits, loss of revenue, loss of interest and third-party claims, may not be claimed. Loss or damage to data and costs of recovery or data recovery is considered to be indirect loss.

The above limitation of liability does not include gross negligence and deliberate acts, as they do not apply if they are in violation of mandatory/absolute legislation.

APPENDIX E: DEVIATIONS FROM STANDARD CLAUSES

On behalf of Data Processor,	***On behalf of the Data Controller,***
Date:	**Date:**
Signature:	**Signature:**
Name:	**Name:**
Title:	**Title:**