Data Processing Agreement

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 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 subprocessor(s). If the Customer objects to the appointment of a new sub processor 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;

4. Transfer the processing of personal data to a subprocessor in a third country;

    a. have the personal data processed in by the Data Processor in a third country.

5. 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.

6. 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 48 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. On termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires storage of the personal data.

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.7. and C.8.

3. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

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.4., 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:

Name:	**Name:**
Position:	**Position:**
Phone number:	**Phone number:**
Email:	**Email:**

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

15. 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. Sub processors changes are subject to chapter 6.3 and Appendix B.2.

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.

16. Appendix A: Information about the processing

16.1.

16.2. A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

16.2.1. A.1.1 Brand Protection

- *Anti-Phishing:* Not applicable. No processing of personal data.
- *Dark Web Monitor:* Collecting data in open and closed forums based on keywords provided by the Data Controller.
- *Rogue App Monitor:* Not applicable. No processing of personal data.
- *Typo Squat Monitor:* Not applicable. No processing of personal data.

16.2.2. A.1.2 Consulting

- *AD Health Check:* See 'A.1.5 Software, Chronos'.
- *Assume Breach Test (Internal Penetration Test):* Data Processor performs an attack similar to what a malicious actor could do, against the Data Controller's systems. During such an attack, the Data Processor can potentially gain access to any data in the Data Controller's systems. The purpose of the assignment is determining whether data can be accessed and not to actually use the data.
- *Compromise Assessment:* See 'A.1.5 Software, Chronos'.
- *Emergency Response:* See 'A.1.5 Software, Chronos'.
- *Emergency Response Retainer Agreement:* When this agreement takes effect and Emergency Response is initiated utilizing the 'A.1.5 Software, Chronos', the purpose of Data Processor's processing of personal data is thorough investigation of artifacts collected. Also see 'A.1.2 Consulting Emergency Response'.
- *GAP Analysis:* Not applicable. No processing of personal data.

16.2.3. A.1.3 Financial Fraud Data Recovery

- *Credit Cards:* Data Controller uses CSIS' Credit Cards solution to collect, identify, and present detected compromised Credit Cards for the Data Controller.

- *Customer Credentials:* Data Controller uses CSIS' Customer Credentials solution to collect, identify, and present detected compromised Customer Credentials for the Data Controller.
- *Money Mules:* Money mule accounts are bank accounts used by cybercriminals to store stolen funds before transfer to destination. When uncovering such an account, it will be shared with all customers subscribing to the service to make sure that any in- or outbound transactions are flagged.
- *Threat Detection and Response:* Data Controller uses CSIS' Managed Detection and Response service to help prevent, detect, and respond to advanced security threats and risks within their IT environment. As a part of the service a range of CSIS' internal tools may be used; see 'A.1.5 Software, Chronos' for more details.

16.2.4. A.1.4 Managed Detection and Response

- *Threat Detection and Response:* Data Controller uses CSIS' Managed Detection and Response service to help prevent, detect, and respond to advanced security threats and risks within their IT environment. As a part of the service a range of CSIS' internal tools may be used; see 'A.1.5 Software, Chronos' for more details.

16.2.5. A.1.5 Software

- *Chronos:* Data Processor uses the Chronos investigations platform to look for threats, risks, or security baseline issues by extracting system metainformation such as diagnostic logs, application compatibility databases, cryptographic hashes of files, visited URLs in browsers, DNS caches and other similar datasets.

16.2.6. A.1.6 Targeted Threat Identification

- *Employee Credentials:* Data Controller uses CSIS' Employee Credentials solution to collect, identify, and present detected compromised Employee Credentials for the Data Controller.
- *HoneyNet Monitor:* Not applicable. No processing of personal data.
- *Trojan Monitor:* Not applicable. No processing of personal data.

16.2.7. A.1.7 Threat Feeds (Cyber Defence Feeds)

- *Malware and C2 Feeds:* Not applicable. No processing of personal data.
- *Threat Insights:* Not applicable. No processing of personal data.

16.3. 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):

16.3.1. A.2.1 Brand Protection

- *Anti-Phishing:* Not applicable. No processing of personal data.
- *Dark Web Monitor:* The nature of the processing is to detect possible compromised data belonging to the Data Controller. This is done by monitoring the activities in open and closed forums on the Internet. The detected data is identified and then released for final confirmation.
- *Rogue App Monitor:* Not applicable. No processing of personal data.
- *Typo Squat Monitor:* Not applicable. No processing of personal data.

16.3.2. A.2.2 Consulting

- *AD Health Check:* See 'A.2.5 Software, Chronos'.
- *Assume Breach Test (Internal Penetration Test):* See 'A.1.5 Consulting, Assume Breach Test'.
- *Compromise Assessment:* See 'A.2.5 Software, Chronos'.
- *Emergency Response:* Data processing of all the collected data to find Indicators of Compromise within then system. Both manual and automated analysis need, see A.1.5 Software.
- *Emergency Response Retainer Agreement:* Should the Retainer Agreement take effect, all processing will be as found in 'A.2.2 Consulting, Emergency Response'.
- *GAP Analysis:* Not applicable. No processing of personal data.

16.3.3. A.2.3 Financial Fraud Data Recovery

- *Credit Cards:* The nature of the processing is to detect possible compromised credit cards belonging to the Data Controller. This is done by monitoring the activities of malicious actors operating on the Internet. The detected data is matched against predefined search strings belonging to the Data Controller and then released for final confirmation.
- *Customer Credentials:* The nature of the processing is to detect possible compromised credentials belonging to the customers of the Data Controller. This is done by monitoring the activities of malicious actors operating on the Internet. The detected data is matched against pre-defined search strings belonging to the Data Controller and then released for final confirmation.
- *Money Mules:* Data processing of IBAN/SWIFT, account name, sort code and country code when available.

16.3.4. A.2.4 Managed Detection and Response

- *Threat Detection and Response:* The nature of the processing is to store and process data identified in leaks or forensics investigations and hereby personal and sensitive data *could* be made available for the Data Controller, since the content of a leak and potential data collected in forensics is not known beforehand. As a part of the service a range of CSIS' internal tools may be used; see 'A.2.5 Software, Chronos' for more details.

16.3.5. A.2.5 Software

- *Chronos:* Finding intruder activity and Indicators of Compromise in the extracted data via both automated and manual investigation of data. Some indicators may be cross referenced with OSINT (Open-Source Intelligence) Tools.

16.3.6. A.2.6 Targeted Threat Identification

- *Employee Credentials:* The nature of the processing is to detect possible compromised credentials belonging to the employees of the Data Controller. This is done by monitoring the activities of malicious actors operating on the Internet. The detected data is matched against pre-defined search strings belonging to the Data Controller and then released for final confirmation.
- *HoneyNet Monitor:* Not applicable. No processing of personal data.
- *Trojan Monitor:* Not applicable. No processing of personal data.

16.3.7. A.2.7 Threat Feeds (Cyber Defense Feeds)

- *Malware/C2 Feeds:* Not applicable. No processing of personal data.
- *Threat Insights:* Not applicable. No processing of personal data.

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

16.4.1. A.3.1 Brand Protection

- *Anti-Phishing:* Not applicable. No processing of personal data.
- *Dark Web Monitor:* Any data collected based on keywords e.g. credit card information, names, email addresses, usernames, and passwords.
- *Rogue App Monitor:* Not applicable. No processing of personal data.
- *Typo Squat Monitor:* Not applicable. No processing of personal data.

16.4.2. A.3.2 Consulting

- *AD Health Check:* See 'A.3.5 Software, Chronos'.
- *Assume Breach Test (Internal Penetration Test):* The assignment simulates what a real attacker might do, and therefore the data processor can potentially access (process?) any type of personal data.
- *Compromise Assessment:* See 'A.3.5 Software, Chronos'.
- *Emergency Response:* Data subjects would include what can be found in 'A.3.4 Managed Detection and Response', 'A.3.5 Software, Chronos'. Dependent on the scope of the case, any data found in the compromised system could be subject to processing.
- *Emergency Response Retainer Agreement:* See 'A.3.2 Consulting, Emergency Response'.
- *GAP Analysis:* Not applicable. No processing of personal data.

16.4.3. A.3.3 Financial Fraud Data Recovery

- *Credit Cards:* Data Controller's employees and customer's credit card information.
- *Customer Credentials:* Data Controller's customer's names, email addresses, usernames, and passwords.
- *Money Mules:* Data processing of IBAN/SWIFT, account name, sort code and country code when available.

16.4.4. A.3.4 Managed Detection and Response

- *Threat Detection and Response:* Data types are dependent on the alert generated by the Data Controllers system. The regular data provided from Data Controllers systems are IP addresses, names, e-mails addresses, usernames, domain names, computer names and browsing history. As a part of the service a range of CSIS' internal tools may be used; see 'A.3.5 Software, Chronos' for more details.

16.4.5. A.3.5 Software

- *Chronos:* The ordinary personal data is IP addresses, names, e-mail addresses, and bank account numbers. Dependent on the use-case any metadata present on the device can be included; see 'A.3.5 Software, Chronos' for more details.

16.4.6. A.3.6 Targeted Threat Identification

- *Employee Credentials:* Data Controller's employees names, email addresses, usernames, and passwords.
- *HoneyNet Monitor:* Not applicable. No processing of personal data.
- *Trojan Monitor:* Not applicable. No processing of personal data.

16.4.7. A.3.7 Threat Feeds (Cyber Defense Feeds)

- *Malware/C2 Feeds:* Not applicable. No processing of personal data.
- *Threat Insights:* Not applicable. No processing of personal data.

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

16.5.1. A.4.1 Brand Protection

- *Anti-Phishing:* Not applicable. No processing of personal data.
- *Dark Web Monitor:* See 'A.3.1 Brand Protection, Dark Web Monitor'.
- *Rogue App Monitor:* Not applicable. No processing of personal data.
- *Typo Squat Monitor:* Not applicable. No processing of personal data.

16.5.2. A.4.2 Consulting

- *AD Health Check:* See 'A.4.5 Software, Chronos'.
- *Assume Breach Test (Internal Penetration Test*): Depending on the systems included in the scope of the assignment, any type of data can potentially be accessed/processed.
- *Compromise Assessment:* See 'A.4.5 Software, Chronos'.
- *Emergency Response:* Data categories would include what can be found in A.3.4 Managed Detection and Response and A.3.5 Software. Dependent on the scope of the case, any data found in the compromised system could be subject to processing.
- *Emergency Response Retainer Agreement*: See 'A.4.2 Consulting, Emergency Response'.
- *GAP Analysis:* Not applicable. No processing of personal data.

16.5.3. A.4.3 Financial Fraud Data Recovery

- *Credit Cards:* Data Controller's employees and customers who had their credit card information compromised.
- *Customer Credentials:* Data Controller's customers who had their credentials compromised.
- *Money Mules:* Data processing of IBAN/SWIFT, account name, sort code and country code when available.

16.5.4. A.4.4 Managed Detection and Response

- *Threat Detection and Response:* Any employees at the Data Controller. As a part of the service a range of CSIS' internal tools may be used; see 'A.4.5 Software, Chronos' for more details.

16.5.5. A.4.5 Software

- *Chronos:* Data Controller's employees who are in scope of an assignment defined by Data Controller. See 'A.4.5 Software, Chronos'.

16.5.6. A.4.6 Targeted Threat Identification

- *Employee Credentials:* Data Controller's employees who had their credentials compromised.
- *HoneyNet Monitor:* Not applicable. No processing of personal data.
- *Trojan Monitor:* Not applicable. No processing of personal data.

16.5.7. A.4.7 Threat Feeds (Cyber Defense Feeds)

- *Malware/C2 Feeds:* Not applicable. No processing of personal data.
- *Threat Insights:* Not applicable. No processing of personal data.

16.6. A.5. 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.

17. Appendix B: Authorized subprocessors

17.1. B.1. Approved subprocessors

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

Name	Amazon Web Services - Dansk filial af Amazon Web Services EMEA SARL, Luxembourg	Google Cloud - Google Cloud
VAT no.	DK39009323	IE3668997OH
CVR	39009323	
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.

17.2. B.2. Prior notice for the authorisation of sub-processors

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

If the Customer objects to the appointment of a new sub processor 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.

18. Appendix C: Instruction pertaining to the use of personal data

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

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

18.1.1. C.1.1 Brand Protection

- *Anti-Phishing:* Not applicable. No processing of personal data.
- *Dark Web Monitor:* Data processing of all the collected data to find compromised information.
- *Rogue App Monitor:* Not applicable. No processing of personal data.
- Typo Squat Monitor: Not applicable. No processing of personal data.

18.1.2. C.1.2 Consulting

- *AD Health Check:* See 'A.4.5 Software, Chronos'. • Assume Breach Test (Internal Penetration Test): See 'A.1.2 Consulting, Assume Breach Test'
- *Compromise Assessment:* See 'A.4.5 Software, Chronos'.
- *Emergency Response:* Data processing of all the collected data to find Indicators of Compromise within then system. Both manual and automated analysis need, see A.1.5 Software.
- *Emergency Response Retainer Agreement:* When this agreement takes effect and Emergency Response is initiated utilizing the C.1.5 Software, the instruction for Data Processor's processing of personal data is to enable thorough investigation of artifacts collected. Also see: C.1.2 Consulting Emergency Response.
- *GAP Analysis:* Not applicable. No processing of personal data.

18.1.3. C.1.3 Financial Fraud Data Recovery

- *Credit Cards:* Collect, identify, and present detected compromised Credit Cards for the Data Controller in the Threat Intelligence Portal.

- *Customer Credentials:* Collect, identify, and present detected compromised Customer Credentials for the Data Controller in the Threat Intelligence Portal.
- *Money Mules:* Data processing of IBAN/SWIFT, account name, sort code and country code when available.

18.1.4. C.1.4 Managed Detection and Response

- *Threat Detection and Response:* Analyse IT security alerts generated by the Data Controller's systems and investigate where applicable. As a part of the service a range of CSIS' internal tools may be used; see 'C.1.5 Software, Chronos' for more details.

18.1.5. C.1.5 Software

- *Chronos:* Finding intruder activity and Indicators of Compromise in the extracted data via both automated and manual investigation of data. Some indicators may be cross referenced with OSINT (Open-Source Intelligence) Tools. See 'C.1.5 Software, Chronos'.

18.1.6. C.1.6 Targeted Threat Identification

- *Employee Credentials:* Collect, identify, and present detected compromised Employee Credentials for the Data Controller in the Threat Intelligence Portal.
- *HoneyNet Monitor:* Not applicable. No processing of personal data.
- *Trojan Monitor:* Not applicable. No processing of personal data.

18.1.7. C.1.7 Threat Feeds

- *Malware Feeds:* Not applicable. No processing of personal data.
- *Threat Insights:* Not applicable. No processing of personal data.

18.2. C.2. 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.

18.3. C.3. 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.2.

18.4. C.4. 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.

18.5. C.5. 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)
- CSIS Security Group (Remote working via Virtual Private Networking)
- AWS Europe (Frankfurt, Germany)
- GCP Europe (Belgium, Finland, Ireland, Netherlands)

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

The Data Processor is entitled within the framework of the Clauses to perform transfers to third countries if this is deemed necessary for support and operative reasons (e.g. AWS and GCP support), however the Data Processor cannot do so without the Data Controller's approval.

18.7. C.7. 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 the following types of reports may be used in compliance with the Clauses:

- ISAE 3000
- 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.

18.8. C.8. Procedures for audits, including inspections, of the processing of personal data being performed by subprocessors

The Data Processor commits to obtaining a report as set out in Clause C.7 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 obtained:

- 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 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. 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.

19. 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.

20. 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:**