Changelog

VERSION	DATE	AUTHOR (INITIALS)	CHANGES	APPROVED BY
1.1.	x	The Danish Data Protection Agency	Clauses 9.2. and 10.4., *(Corrected cross-references).*	Intect
1.2	x	The Danish Data Protection Agency	Clause 7.6 (*now made optional and amended wording*)	Not implemented
1.2	01-05-2026	Intect (SK)	Published	Intect Management
1.25	01-08-2025	Intect (SK)	Amendments to: - The Parties and signatures have been moved to the beginning of the document - Section 9 (Use of Sub-processors) - Section 13 (Deletion and Return of Data) - Insertion of Clause 15.2 - Appendices A, B, and C updated in their entirety	Intect Management
1.26	01-10-2026	Intect (SK)	Amendments to: - Design Added the following: - 4.3 - 11.2 - A3.1 - C.4. 5 – Legal retention - C.7. 1., 2., 7., 8. ,12., 14., 17 – Audit Change of wording - 2.4 - B.1 – link to sub-processors via Trust Center - D.1-4.	Intect Management

Standard Contractual Clauses

1. For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) this Data Processing Agreement is entered into between Intect ApS, CVR No. 37035084 (hereinafter referred to as the "Data Processor"), and the Customer who has entered into an agreement with Intect for the use of Intect's services (hereinafter referred to as the "Data Controller"), each individually referred to as a "Party" and collectively as the "Parties".

2. HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Signatures

3. This Data Processing Agreement is entered into and signed electronically as part of the establishment of the contractual relationship between the Customer and Intect.

4. The Customer's electronic acceptance of this Data Processing Agreement constitutes the Customer's signature to the Agreement.

Data controller and data processor contacts/contact points

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

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

DATA PROCESSOR
Navn: Signe K.
Stilling: Intect, DPO
Telefonnummer: +45 71 99 11 22
E-mail: dpo@intect.io

1. Table of Contents

Data controller and data processor contacts/contact points 2
2. Preamble 4
3. The rights and obligations of the data controller 5
4. The data processor acts according to instructions 5
5. Confidentiality 5
6. Security of processing 5
7. Use of sub-processors 6
8. Transfer of data to third countries or international organisations 7
9. Assistance to the data controller 8
10. Notification of personal data breach 9
11. Erasure and return of data 9
12. Audit and inspection 9
13. The parties' agreement on other terms 10
14. Commencement and termination 10
Appendix A Information about the processing 11
Appendix B Authorised sub-processors 13
Appendix C Instruction pertaining to the use of personal data 14
Appendix D The parties' terms of agreement on other subjects 21

2. Preamble

1. This Agreement is based on the Danish Data Protection Agency's(DDPA) standard contractual clauses (SCC) for data processing agreements and has been adapted to support the Parties' compliance with applicable data protection legislation.

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

3. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Services:

4. The data processor will deliver the services described in the Main Agreement and/or the general terms between the parties and will in order to fulfil the Main Agreement, process personal data on behalf of the data controller in accordance with the Clauses.

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

Appendices:

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

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.
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.
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.
APPENDIX D	Contains provisions for other activities which are not covered by the Clauses.

Storage of the Data Processing Agreement

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

Compliance with Applicable Law

8. 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.

3. The rights and obligations of the data controller

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

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

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

Processing of personal data

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.

2. 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.

3. The handling of unlawful instructions is addressed in C.1.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

2. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

Demonstration of Employee Confidentiality Obligation

3. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

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

a. Pseudonymisation and encryption of personal data;

b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

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

The Data Processor's Responsibility under Article 32

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

The Data Processor's Assistance to the Data Controller in Relation to Article 32

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

7. Use of sub-processors

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

Prior general written Authorisation from the Data Controller

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior **GENERAL WRITTEN AUTHORISATION** of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least **14 CALENDAR 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).

The list of sub-processors (ROSP)

4. The list of sub-processors already authorised by the data controller can be found in Appendix B.

Obligations of Sub-processors

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. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

Transfer of personal data

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.

Transfer of Data pursuant to EU Law or the National Law of the Member States

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

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

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

   c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

Responding to Requests for the Exercise of Right

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

Obligation to assist with appropriate measures

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than **72 HOURS** after having become aware of it, notify the personal data breach to the competent supervisory authority, **The Danish Data Protection Agency** (Datatilsynet), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, **The Danish Data Protection Agency** (Datatilsynet), 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.

Specification of the appropriate Technical and Organisational Measures

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

Timeframe for Notification

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.

Assistance with Notification of Personal Data Breaches

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

11. Erasure and return of data

Erasure or Return

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to **DELETE** all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

2. Erasure or Return is addressed in Appendix C.4.

12. Audit and inspection

Information to be Make Available

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.

Access to the Data Processor's Facilities

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

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

Commencement

1. The Clauses shall become effective on the date THE MAIN AGREEMENT is signed and entered into, by both parties.

Renegotiation

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 Parties undertake, in good faith, to discuss any objections and strive to find a mutually acceptable solution through renegotiation of the Data Processing Agreement.

4. The Parties shall have the right to terminate the Agreement with effect from the desired effective date, if the changes cannot be accepted. Neither Party shall have any claims against the other in this respect

Duration

5. 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.

6. This Data Processing Agreement shall remain in effect for as long as the Data Processor processes Personal Data on behalf of the Data Controller in accordance with the MAIN AGREEMENT.

Termination

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

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:

1. The Data Processor shall make software-as-a-service (SaaS) solutions ("Services") available to the Data Controller and its employees on a subscription basis. The Services may be accessed either via the Data Processor's website or through the Data Processor's applications.

2. The Data Controller's use of the Data Processor's cloud-based Services shall take place by means of the Data Controller's self-service through the Data Processor's website and/or via the Data Processor's app. The Data Controller's employees may likewise access their own information, such as payslips, absence records, holiday overviews, and documents uploaded by the employee or the customer, for example, an employment contract. Both the Data Controller's and its employees' use requires a user ID and a unique password.

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):

1. The Data Processor shall process Personal Data on behalf of the Data Controller as part of the delivery of the Data Processor's Services.

2. The Data Processor's processing of Personal Data primarily concerns the handling of Services relating to the Data Controller's:

    a) Payroll administration
    b) HR administration
    c) Data integration / consolidation / BI

3. In addition, the Data Processor shall be responsible for operation, testing, maintenance, development, and error correction of the Services provided.

4. Processing may include any handling of Personal Data, including collection, registration, organisation, structuring, storage, adaptation or alteration, retrieval, search, disclosure by transmission, dissemination or any other form of disclosure, combination or alignment, restriction, erasure or destruction, including support.

5. The Data Processor shall collect, store, analyse, and use Personal Data concerning both the Data Controller and its customers for the purpose of issuing invoices, receiving payment information from payment intermediaries, and disclosing relevant information to the Data Controller.

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

1. All personal data which the data processor is given access to, shall be treated confidentially.

2. The types of Personal Data processed through the Application depend on the individual customer and the end-user's use.

3. Processing of **special categories** of Personal Data pursuant to Article 9 of the GDPR shall only take place if the customer or end-user independently chooses to enter such information into the Application, which shall be under the customer's full responsibility and control. The Application is not designed or intended for the pro-cessing of special categories of data. However, it cannot be excluded that end-users or the customer may enter such information in free-text fields.

4. The types of Personal Data processed in connection with the provision of the Service, and the processing of Personal Data via the Application, therefore vary depending on usage.

5. The Personal Data processed by the Data Processor in connection with the Data Controller's use of the Data Processor's Services will differ depending on the category of the Data Subject, as set out in the following overview:

CATEGORIES OF DATA SUBJECTS	PERSONAL DATA (PII)
Customers (Data Controller)	• Contact persons at the Data Controller, including their contact details such as phone, email, title, department, address • Business Registration Number (CVR)
Current and former employees of the Data Controller	Ordinary data: Identification data: • Name, address, phone number, date of birth, email – private and work, employee ID, customer number Other data: • Workplace and employment details • Photo • Car • Language preference • Time and absence records Confidential data: • Personal Identification Number (CPR) • Information on criminal matters, including criminal record • Passport and driver's licence • Information on social issues Financial data: • Payment card details, tax, holiday settlement, pension settlement, bank account, payroll data
Partners	• Name • Address • Business Registration Number (CVR) • Contact details • Contact persons in Support, including their contact details such as phone, email, title, department, address
Data related to user activity	• IP addresses, audit trails, and log data • Purchase history • Cookie ID

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

1. See overview above, A3.

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:

1. This Data Processing Agreement shall remain in effect for as long as the Data Processor processes Personal Data on behalf of the Data Controller in accordance with the MAIN AGREEMENT.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

1. Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

2. The Data Processor shall maintain a current list of authorised sub-processors on its website at The Data Controller acknowledges and agrees that publication of updates to such list on the website shall constitute notice of changes to sub-processors for the purposes of this Agreement.

3. Updates to the list will be published on the website and notified to the Data Controller by e-mail or other agreed communication channel.

4. The list of sub-processors already authorised by the data controller can be found on Intect Trust Centre (sub-processors)

5. Upon commencement of the Clauses, the Data Controller has approved the use of the listed sub-processors for the described processing activity.

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

1. The data processor has the data controller's **GENERAL AUTHORISATION** for the engagement of sub-processors, in accordance with Clause 7.2.

2. Any notification required under this Agreement shall be provided in accordance with Clause 7.3.

3. For the sake of clarity (from 7.3);

   > The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least **14 CALENDAR 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).

4. The Data Processor shall thereby give the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

5. The Data Controller acknowledges that the Data Processor's Services are standardized, cloudbased subscription services made available to a large number of customers, and that the Data Processor, as a general rule, is therefore not able to accommodate individual requests to opt out of specific Sub-processors.

6. If the Data Controller objects to the addition of a new Sub-processor, the Data Processor undertakes to assess the objection loyally and in good faith and to examine whether reasonable technical or commercial alternatives exist. If it is not possible to accommodate the objection, the Data Controller shall be entitled to terminate the MAIN AGREEMENT with immediate effect. Neither Party shall have any claim against the other as a result thereof.

7. In case the Data Controller has not objected to the change of a sub-processor or engagement of a new sub-processor within the deadline, the sub-processor is seen as accepted.

8. Should the change to the list of sub-processors include an addition of sub-processor in a third country, the Data Controller must be notified as agreed in appendix C, clause C.6.

Obligations of Sub-processors

9. A Data Processing Agreement (DPA) shall be entered into with all relevant sub-contractors, specifying their obligations and responsibilities under data protection legislation.

10. The Data Processor shall implement a process ensuring that all suppliers and Sub-processors continue to comply with the requirements of the Agreement.

11. A supervision plan shall be prepared to ensure that relevant Sub-processors are subject to appropriate monitoring

Use of Global Supplier

12. If a global supplier, such as Microsoft, Google or Amazon, is used as a Sub-processor, the Data Controller accepts that the terms and conditions in force at any given time, as agreed between the Parties and the global supplier, shall constitute the basis for the global supplier's processing of the Data Controller's data, including in relation to requirements for inspection, audit, control, documentation, and liability.

13. Links to the most recent terms and conditions for these Sub-processors can be found on the global supplier's website.

Appendix C Instruction pertaining to the use of personal data

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

1. The Data Processor's processing of Personal Data on behalf of the Data Controller shall take place through the processing activities described in Appendix A.

Instruction on the Use of Third-Party App(s)

2. The Services are developed with an open API, which enables others to develop and offer apps that can communicate with the Application, including the exchange of information across the programs ("Third-Party App(s)"). To the extent that the Data Controller chooses to install and use Third-Party Apps that can communicate with the Application, this shall be deemed to constitute an instruction to the Data Processor permitting the transfer of information entered/uploaded into the Application as well as information generated by the Application to such Third-Party Apps.

3. The Data Controller further accepts that its Employees may install and use Third-Party Apps that can communicate with and exchange the individual Employee's access to information with the Application, and that such data processing shall be covered by the instruction under this Agreement.

Notification of Unlawful Instructions

4. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. If the Data Processor is of the opinion that the execution of an instruction from the Data Controller will, in all probability, be contrary to applicable law, the Data Processor shall immediately notify the Data Controller thereof. If the Data Controller maintains that the instruction is in compliance with applicable law and

insists that the instruction be carried out, the Data Processor may execute the instruction without incurring liability towards the Data Controller, and the Data Controller shall indemnify the Data Processor against any third-party claims, including claims from data subjects, resulting from the executed instruction.

6. Notwithstanding with above the Data Processor shall not be obliged to actively verify or investigate the legality of the Data Controller's instructions.

7. To the extent that the Data Controller issues instructions to the Data Processor that subsequently prove to be unlawful, the Data Controller shall indemnify the Data Processor against any loss resulting therefrom, including indemnifying the Data Processor against any claim brought against the Data Processor as a result thereof, including fines or other sanctions from relevant authorities, as well as claims from other third parties, including the affected data subjects, sub-processors, and the Data Processor's other business partners.

C.2. Security of processing

1. The Data Processor shall be obliged to implement all necessary technical and organisational measures in accordance with Article 32 of the GDPR in order to ensure a high level of security.

2. The measures shall take into account the current state of the art, the costs of implementation, as well as the nature, scope, context, and purposes of the processing, and the risks posed by the processing to the rights and freedoms of data subjects.

3. The Data Processor shall, however, continuously evaluate these measures and ensure compliance with **ISAE 3000** or an equivalent framework.

4. The Data Processor shall therefore be entitled and obliged to decide which technical and organisational security measures must be implemented to establish the necessary (and agreed) level of security.

5. If the Data Controller requests information regarding security measures, documentation, or other types of information about how the Data Processor processes Personal Data, and such requests go beyond the standard information normally made available by the Data Processor to comply with applicable data protection legislation, and such requests result in additional work for the Data Processor, the Data Processor shall be entitled to request payment from the Data Controller for such additional work.

6. The Data Processor shall, however, in all circumstances and at a minimum, implement the following measures as agreed with the Data Controller:

TECHNICAL MEASURES	DESCRIPTION
Access Control	Access to Personal Data and systems is restricted on a need-to-know basis, ensuring that only employees with a work-related requirement have access to the relevant data. Access rights are granted individually and are reviewed on an ongoing basis to ensure that they are up to date and appropriate in relation to the employee's work tasks. All users have unique access credentials in the form of individual usernames and passwords, which are created and managed in accordance with generally accepted security principles. Two-Factor Authentication (2FA/MFA) is used where possible to strengthen security. Access to Personal Data is furthermore restricted to authorised employees who have been instructed to act in accordance with the customer's instructions and applicable data protection legislation.

Cryptography	The Data Processor shall ensure that sensitive Personal Data is always protected against unauthorised access during transfer and storage. All communication involving sensitive Personal Data shall take place over secure, encrypted connections. If such data is transferred outside the Data Processor's controlled network, it shall at a minimum be protected by strong encryption. Where relevant and feasible, the Data Processor shall also apply pseudonymisation or anonymisation to limit the risks associated with processing and storing Personal Data.
Operational Security	The Data Processor shall ensure that appropriate operational security is implemented to protect systems and data against threats such as viruses, malware, and unauthorised access. This includes the following measures: • Antivirus • Physical firewall • Centralised user and group management • Monitoring • VPN • Patching • Use of secure connections • Separate administrator accounts Procurement, development, and maintenance of systems: • Secure development process Data Storage and Encrypted Backup • Onsite backup (point-in-time) • Offsite backup • Backups are encrypted
Communication Security	Protection and segmentation of networks Established secure communication methods
Management of Information Security Incidents and Personal Data Breaches	The Data Processor shall implement an incident response plan for the effective handling of personal data breaches. This process shall ensure that all incidents are identified, assessed, and handled promptly and correctly. There shall also be a process for notifying the Data Controller, ensuring that the Data Controller is informed without undue delay and that all necessary information regarding the incident is provided, including its scope, risks, and the measures taken.
Audit logs	Audit logs shall be maintained regarding system access and activities, including log data. All changes relating to the processing of Personal Data shall also be logged. Active system logs must be maintained on all endpoint devices as

	well as servers to ensure that all relevant activities are monitored and can be verified if necessary.

ORGANIZATIONAL MEASURES	DESCRIPTION
Information Security Policies	Overall guidelines and requirements for information security.
Organisation of Information Security	The Data Processor has appointed a Data Protection Officer (DPO). Employees, customers, and other stakeholders may contact Intect's Data Protection Officer at dpo@intect.io. In addition, a Compliance Team has been established, tasked with monitoring and managing data protection within Intect.
Employee Security	The Data Processor has established procedures to ensure that employees processing Personal Data are suitable and trustworthy. This includes: • Background checks, including review of criminal records where relevant, prior to employment in relevant positions. • All employees sign confidentiality agreements. • Employees undergo regular GDPR awareness training in information security and data protection to ensure understanding and compliance with applicable rules and internal policies. • Established procedures for the employee lifecycle.
Physical and Environmental Security	The Data Processor undertakes to maintain appropriate physical and environmental security at the locations where Personal Data is processed or stored, including data centres and any office addresses. Access to physical premises where Personal Data is processed shall be restricted to authorised individuals and protected through access control systems such as key cards, alarms, surveillance, or equivalent mechanisms. The Data Processor shall ensure that physical access points, including main entrances, server rooms, and other relevant areas, are protected against unauthorised access, intrusion, and environmental impacts such as fire, water, and power disturbances. To the extent that physical or environmental security is wholly or partly outsourced to a third party, the Data Processor undertakes to ensure that such subcontractors comply with equivalent security levels and requirements as set out in this Agreement and applicable data protection legislation.
Asset Management	The Data Processor has implemented policies for the secure handling, storage, and maintenance of all physical equipment to minimise the risk of data loss and unauthorised access. The Data Processor maintains an inventory of IT equipment used for the processing of Personal Data. Upon termination of employment, equipment must be returned and

	inspected. All data on returned equipment shall be erased in accordance with internal policies, and equipment permanently decommissioned shall be securely destroyed and data erased. Equipment must be stored securely outside working hours and during transport. All access to networks and systems from devices is centrally managed. Lost or stolen equipment must be reported immediately, after which appropriate security measures shall be implemented, including remote wiping.

C.3. Assistance to the data controller

1. The Data Processor shall, to the extent possible – within the scope and extent set out below – assist the Data Controller in accordance with this Agreement by implementing such technical and organisational measures as may support the Data Controller's ability to respond to requests for the exercise of data subjects' rights

2. If the Data Controller requests the Data Processor's assistance with the services described in Clause 9.2 (c), (d) and (e), the Data Processor shall make itself available for such assistance. To the extent that the assistance exceeds what can reasonably be regarded as customary and expected, the Data Processor shall be entitled to charge a reasonable remuneration for such assistance. The remuneration shall be determined on the basis of the time spent and in accordance with the applicable hourly rates in force at any given time as set out in the Data Processor's General Terms and Conditions

C.4. Storage period/erasure procedures

1. Upon termination of the Services relating to the Processing of Personal Data, the Data Processor shall be obliged to delete all Personal Data processed on behalf of the Data Controller, provided that the Data Processor has received a **WRITTEN INSTRUCTION** to delete from the Data Controller.

2. As a general rule, the Data Processor shall act in accordance with the instructions of the Data Controller and shall not delete Personal Data without a prior, explicit, and written instruction. However, deletion may take place without a separate instruction if required by the Data Processor's General Terms and Conditions, as agreed between the Parties and in force at any given time. It shall therefore be the responsibility of the Data Controller, as a general rule, to submit a written instruction if deletion is to be carried out in accordance with Clause 11.1.

3. When deletion has been carried out in accordance with an instruction, the Data Processor shall confirm such deletion in writing to the Data Controller.

4. If the Data Processor does not receive a written instruction to delete Personal Data, the Data Processor shall contact the Data Controller to request such instruction. If no response is received from the Data Controller within a reasonable time frame, the Data Processor shall delete the Personal Data in accordance with the applicable rules and provisions of the GDPR.

   Legal retention obligation

5. As a Data Processor, Intect process and retain Personal Data solely on behalf of and under the instructions of the Data Controller.

C.5. Processing location

1. The processing of Personal Data covered by these Clauses shall take place at the Data Processor's own premises as well as at approved Sub-processors.

2. The Data Controller hereby instructs that Personal Data may be processed by the Sub-processors listed in the Trust Centre at commencement, as well as at the locations specified therein.

3. The Data Controller hereby accepts the processing of Personal Data may also take place through remote work, provided that such processing is carried out in accordance with the Data Processor's internal remote work policy.

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

1. The Data Processor shall seek to ensure that Personal Data is processed and stored within the EU/EEA. As a general rule, transfers of Personal Data outside the EU/EEA shall not take place.

2. In certain cases, Personal Data may be transferred to Greenland, but solely in relation to the processing of data concerning Greenlandic companies and in accordance with the instructions of the Data Controller.

3. Sub-processors in Greenland shall only be involved in the processing of data for Greenlandic companies and shall comply with the relevant data protection requirements applicable to such processing.

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

1. The Data Controller may not conduct more than one audit in any twelve-month period unless:
   a) required by applicable law;
   b) following a Personal Data Breach; or
   c) where the Data Controller has reasonable grounds to suspect material non-compliance with this Agreement.

2. The costs incurred by the Data Processor in connection with a physical inspection and/or an audit carried out on behalf of the Data Controller at the Data Processor or its Sub-processors shall be borne by the Data Controller. The time of the Data Processor and/or its Sub-processors shall be remunerated in accordance with the hourly rates applied by the Data Processor at any given time, as set out in the Data Processor's General Terms and Conditions.

Audit report

3. The Data Processor shall, annually and without separate remuneration, arrange for the preparation of an audit report concerning the Data Processor's level of information security and the measures implemented by the Data Processor. The audit report shall include a review of the established management systems and a report on their effectiveness as well as the comments of the designated third party.

4. The report shall be prepared by an independent third party concerning the Data Processor's and Sub-processors' compliance with the GDPR, data protection provisions under other EU law or the national law of the Member States, and these Clauses.

5. The Parties agree that the following types of certification may be used in accordance with these Clauses:

6. If an ISO 27001/ISO 27701 or ISAE 3402 auditor's report is requested, this shall be at the expense of the Data Controller.

7. The certificate shall be provided to the Data Controller without undue delay for its information, via the Processors Trust Center.

8. The Data Controller may challenge the framework and/or method of the audit and may, in such cases, request a new audit at **its own expense** under different frameworks and/or by using another method.

9. Based on the results of the audit, the Data Controller shall be entitled to request the implementation of additional measures in order to ensure compliance with the GDPR, data protection provisions under other EU law or the national law of the Member States, and these Clauses.

Access to the Data Processor's Facilities

10. The Data Controller, its representative or representatives acting on behalf of the supervisory authority, upon proper identification, shall be entitled to carry out inspections of the physical facilities and systems from which the Data Processor processes Personal Data.

11. Physical inspections may, however, only take place at the Data Processor's business premises.

12. Before requesting an on-site inspection, the Data Controller shall first review the Data Processor's most recent audit reports, certifications and compliance documentation. On-site audits may only be requested where such documentation does not reasonably address the Data Controller's concerns.

13. To request an inspection, the Data Controller shall submit a detailed inspection plan to the Data Processor no later than **30 CALENDAR DAYS** prior to the proposed inspection date, describing the proposed scope, duration, and starting time of the inspection.

14. The Data Processor shall be obliged to allocate the resources necessary to enable the Data Controller or its advisor/representative to carry out its inspection and/or audit at the Data Processor

15. The Data Controller accepts to bear all costs associated with such inspections and agrees that:

16. In all cases, inspections shall be carried out during normal business hours at the relevant location, in accordance with the Data Processor's policies, and shall not unreasonably interfere with the Data Processor's business operations.

17. The Processor may require the person(s) conducting the audit to be subject to a confidentiality agreement.

18. The remuneration payable to the Data Processor pursuant to the above shall be calculated based on the time spent by the Data Processor in providing the information and on a time and material (T&M) basis, according to the hourly rates specified in the Data Processor's General Terms and Conditions.

19. The Data Processor shall furthermore be entitled to have the Data Controller cover any external costs in-curred by the Data Processor in obtaining the information, including costs of any necessary assistance from Sub-processors.

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

1. Based on a risk assessment, the Data Processor shall obtain annual documentation of relevant Sub-processors' compliance with the GDPR, data protection provisions under other EU law or the national law of the Member States, and these Clauses. The Parties agree that the process for conducting such review, and the sufficiency thereof, shall be documented through the Data Controller's audit of the Data Processor in accordance with Clause C.7.1-9.

2. If additional information regarding Sub-processors' compliance with the GDPR, data protection provisions under other EU law or the national law of the Member States, and these Clauses must be provided to the Data Controller, the Data Processor shall, at the Data Controller's expense and subject to a written agreement, obtain the necessary and available documentation from the Sub-processors.

Appendix D The parties' terms of agreement on other subjects

Version control and precedence of Agreements

1. The data processor reserves the right to continuously make changes to, including clarifications of the agreement. These changes will typically be a result of new recommendations from e.g. The Data Protection Authority or the EU Commission as well as changes in practice and legislation in the area.

2. The Data Controller has, after receiving a notification about a change, **14 WORKDAYS** to object if the change cannot reasonably be accepted.

3. This provision does not apply to changes in the use of sub-data processors, which are regulated in section 7 of the agreement.

Limitation of Liability

1. The parties may agree other clauses concerning the provision of the personal data processing service speci-fying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the funda-mental rights or freedoms of the data subject and the protection afforded by the GDPR.

2. The Data Processor shall be responsible for processing Personal Data in accordance with this Agreement, and applicable data protection legislation, including the General Data Protection Regulation (GDPR). The Data Processor shall only be liable for direct losses suffered by the Data Controller as a result of the Data Processor's material breach of its obligations under this Agreement.

3. The Data Processor's total liability under this Agreement shall be limited to the amount specified in the Data Processors General Terms and Conditions, unless otherwise required by mandatory law.

4. Notwithstanding the foregoing, the limitation of liability shall not apply to the extent that it would result in a restriction of the rights or freedoms of data subjects under the General Data Protection Regulation.