DATA PROCESSING AGREEMENT

Table of Contents

1 PARTIES

1.1 This Data Processing Agreement (DPA), hereinafter referred to as the 'Agreement', is entered into between:

Customer	Supplier
[Name on Company]	Intect aps.
[Adress]	Hørkær 12A
[Postal code + city]	2730 Herlev
CVR: XXXXXX	CVR: 37035084
a company established under the laws of Denmark, hereinafter referred to as the 'Data Controller'	a company established under the laws of Denmark, hereinafter referred to as the 'the Data Processor'

1.2 each a 'party'; together 'the parties' have agreed on the following Standard Contractual Clauses (the 'Clauses') with the purpose of complying with the General Data Protection Regulation and ensuring the protection of privacy as well as the fundamental rights and freedoms of natural persons

2 SIGNATURES

2.1 The Agreement shall be signed by both parties and shall be binding as of the date of signature

2.2 The Agreement signed via ECIT sign.

On behalf of the Data Controller	On behalf of the Data Processor
Name: [Name]	Name: Frants Moraitis
Position: [Position]	Position: Managing Director
Phone number: [+45]	Phone number: +45 71 99 11 22
E-mail: [E-mail]	E-mail: support@intect.io Att: Managing Director

3 CONTACT PERSONS OF THE DATA CONTROLLER AND THE DATA PROCESSOR

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

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

On behalf of the Data Controller	On behalf of the Data Processor
Name: [Name]	Name: Signe K.
Position: [Position]	Position: Intect, DPO
Phone number: [+45]	Phone number: +45 71 99 11 22
E-mail: [E-mail]	E-mail: dpo@intect.io

4 PREAMBLE

4.1 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.

4.2 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 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:

4.3 The Parties have entered into an agreement regarding the Data Controller's use of Intect's Application(s) (the 'Services').

4.4 In the context of the provision of the Services the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

Appendices:

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

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

Storage of the Data Processing Agreement

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

Compliance with Applicable Law

4.8 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.

5 THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

5.1 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.

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

5.3 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.

6 THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

Processing of personal data

6.1 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.

6.2 Such instructions shall be specified in appendices A (Information about the processing) and C (Instruction pertaining to the use of personal data.)

6.3 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 this Agreement.

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

6.4 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.

6.5 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

6.6 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

6.7 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.

6.8 Notwithstanding Clause 6.6, the Data Processor shall not be obliged to actively verify or investigate the legality of the Data Controller's instructions.

6.9 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.

7 CONFIDENTIALITY

7.1 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.

7.2 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

7.3 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.

8 SECURITY OF PROCESSING

8.1 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

8.2 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.

8.3 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;

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

8.4 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.

8.5 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

8.6 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.

8.7 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.

9 USE OF SUB-PROCESSORS

9.1 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

9.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Agreement without the prior general written authorisation of the data controller.

9.3 The data processor has the data controller's **general authorisation** for the engagement of sub-processors.

9.4 The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least **two (2) weeks** in advance.

9.5 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).

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

9.7 The Data Controller acknowledges that the Data Processor's Services are standardized, cloud-based 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.

9.8 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 subscription agreement with immediate effect. Neither Party shall have any claim against the other as a result thereof.

9.9 Use of Global Supplier

9.10 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.

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

Forpligtelser for underdatabehandlere

9.12 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.

9.13 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.

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

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

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

Delivery of the Sub-processor Agreement and any Amendments

9.17 Copies 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.

9.18 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.

10 TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Transfer of personal data

10.1 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

10.2 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.

10.3 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

10.4 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.

10.5 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.

11 ASSISTANCE TO THE DATA CONTROLLER

Responding to Requests for the Exercise of Rights

11.1 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.

11.2 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

11.3 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.

Obligation to assist with appropriate measures

11.4 In addition to the data processor's obligation to assist the data controller pursuant to Clause 8.5., 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 Necessary Technical and Organisational Measures

11.5 Parterne 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.

12 NOTIFICATION OF PERSONAL DATA BREACH

12.1 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

12.2 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.

12.3 Bistand ved anmeldelse af brud på persondatasikkerheden

12.4 In accordance with Clause 11(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.

12.5 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

13 ERASURE AND RETURN OF DATA

Deletion or Return

13.1 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..

13.2 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 13.1.

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

13.4 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.

13.5 The following rules in EU law or the national law of the Member States require the retention of Personal Data after the termination of the Services relating to the Processing of Personal Data, including, but not limited to:

a) **The Danish Bookkeeping Act (Bogføringsloven)**, which requires the retention of accounting material for 5 years from the end of the financial year to which the material relates.

b) **Tax and duty legislation (Skatte- og afgiftslovgivningen),** including rules from the Danish Tax Agency, which may require the retention of information for documentation purposes relating to salaries, fees, and tax matters.

c) **Employment law (Arbejdsretlig lovgivning),** where the retention of certain information may be necessary to document employment relationships and to comply with limitation periods in employment-related disputes.

13.6 The Data Processor shall only be obliged to retain such information to the extent and for as long as necessary to comply with these obligations and may not use the information for any other purpose.

14 AUDIT AND INSPECTION

Information to be Made Available

14.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and this Data Processing Agreement, and shall allow for and contribute to audits, including inspections, conducted by the Data Controller or by another auditor authorized by the Data Controller.

14.2 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 or its Sub-processors.

14.3 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.

14.4 The procedures for the Data Controller's audits, including inspections, with the Data Processor and Sub-processors are further specified in Appendix C to this Data Processing Agreement.

Access to the Data Processor's Facilities

14.5 The Data Processor shall be obliged to grant access to its physical facilities to supervisory authorities which, under applicable law, have access to the facilities of the Data Controller or the Data Processor, or to representatives acting on behalf of the supervisory authority, upon proper identification.

15 THE PARTIES AGREEMENTS ON OTHER SUBJECTS

15.1 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.

15.2 The Data Processor shall be responsible for processing Personal Data in accordance with this Agreement, the instructions, 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 or applicable law. 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. 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.

16 COMMENCEMENT AND TERMINATION

16.1 This Data Processing Agreement shall enter into force on the date of signature by both Parties.

16.2 This Data Processing Agreement shall remain in effect for as long as the service relating to the Processing of Personal Data continues. During this period, this Data Processing Agreement may not be terminated unless otherwise agreed between the Parties in provisions regulating the delivery of the service relating to the Processing of Personal Data.

16.3 Either Party may request that this Data Processing Agreement be renegotiated if changes in legislation or deficiencies in this Data Processing Agreement give rise to such renegotiation.

16.4 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.

16.5 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.

APPENDICES

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. The types of Personal Data processed through the Application depend on the individual customer and the end-user's use.
2. 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 processing of special categories of data. However, it cannot be excluded that end-users or the customer may enter such information in free-text fields.
3. 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.
4. 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:

Tabel 1: Tabel A3 - Behandling af personoplysninger

Categories of Data Subjects	Personal Data
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

B1 APPROVED SUB-PROCESSORS

1. On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:
2. The most recent update of Sub-processors was carried out on: **14-02-2025**

B2 NOTICE PERIOD FOR APPROVAL OF SUB-PROCESSORS

1. The approval period for Sub-processors is set out in Section 9.

General:

Table 2: General sub-processors

Sub-processor	Location	Company ID	Processing activity
ECIT A/S	NO	Rolfsbuktveien 2 1364 Fornebu Norge	Back-office services
ECIT Services A/S	EU	Hørkær 12A, DK-2730 Herlev DK36495022	Development and Support Assistance
ECIT Solutions A/S	DK	Rudolfgårdsvej 1B DK-8260 Viby J Denmark DK28843151	Data Hosting Development and Support Assistance (duplicate – kan evt. fjernes eller flettes med ovenstående) Physical Security
Hubspot Ireland Limited	EU	1 Sir John Rogerson's Quay Dublin 2, Dublin 2, Ireland IE515723	Marketing and Customer Management
JetBrains	EU	Kavčí Hory Office Park, Na Hřebenech II 1718/8, Praha 4 - Nusle, 140 00, Czech Republic	Project Management in Development, including Project Management for 2nd Line Support
Microsoft Ireland Operations Ltd	EU	One Microsoft Place, South County Business Park Leopardstown, Dublin 18, D18 P521 Ireland IE8256796U	Data Hosting in Azure Data Archiving in SharePoint and Email Management
Visma e-conomic A/S	EU	Langebrogade 1, DK1411 København K Denmark DK29403473	Sales Invoicing
ZENDESK Inc.	EU	Njalsgade 72C 1205 København Denmark DK30801830	Customer Support and Engagement
Twilio Inc.	EU	Unter den Linden 10 10117 Berlin Germany IE3335493BH	System Notifications and System Emails.

Intect Payroll

Table 3: Intect Payroll – sub-processors

Sub-processor	Location	Company ID	Processing activity
e-Boks A/S	DK	Hans Bekkevolds Allé 7, DK-2900 Hellerup, DK25674154	Electronic mail primarily for the delivery of payslips to the Data Controller's employees
Skatteforvaltningen	DK	Brændgårdvej 10, DK-7400 Herning, DK19552101	Reporting of personal and payroll data
Danmarks Statistik	DK	Sejrøgde 11, DK-2100 København Ø, DK17150413	Reporting of payroll statistics
POSTNORD STRÅLFORS A/S	EU	Hedegaardsvej 88 DK-2300 København S Denmark DK10068657	Distribution of electronic mail to e-Boks and Kivra in Sweden
Visma LogBuy ApS	DK	Gærtorvet 3 DK-1799 København V Danmark DK29912971	Procurement services specialising in securing discounts through group purchasing (employee benefits).
Mastercard payment services DK A/S	DK	Lautrupbjerg 10, 2750 Ballerup Denmark DK40695869	Requesting money transfers via the customer's bank account and transferring information to the recipient of the money transfer
MDC DATA GREENLAND ApS	GL	Imaneq 1, DK-3900 Nuuk DK21717584	Processing limited to Greenlandic companies
Repenso ApS	GL	Imaneq 30, DK-3900 Nuuk DK12926626	Support for Greenlandic companies

Intect Flow

Table 4: Intect Flow – sub-processors

Sub-processor	Location	Company ID	Processing activity
TS NoCode ApS	DK	Blokken 15 1 DK-3460 Birkerød Denmark DK37114898	Processing software for data management
ECIT Automate ApS	DK	Rudolfgårdsvej 1b DK-8260 Viby J Denmark DK39302284	Support and development of Intect Flow.

Intect Expense

Tabel 5: Intect Expense - sub-processors

Sub-processor	Location	Company ID	Processing activity
ADATO AS	EU	Rolfsbuktveien 2 NO-1364 Fornebu Norway NO:995 221 608	Integration services and processing of expenses and mileage reimbursement.

Intect HR

Tabel 6: Intect HR - sub-processors

Sub-processor	Location	Company ID	Processing activity
Verismo Systems AB	EU	Regeringsgatan 79 111 39 Stockholm, Sweden Org.nr556767-2067	Human Resource Management

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.

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:

Tabel 7: Technical Measures

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.

Tabel 8: Organizational Measures

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.

C.4 STORAGE PERIOD/ERASURE PROCEDURES

1. Upon termination of the Agreement concerning the Processing of Personal Data, the Data Processor shall either delete or return the Personal Data in accordance with Section 11.

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 Appendix B, 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 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.
2. 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.
3. The Parties agree that the following types of certification may be used in accordance with these Clauses:

- ISAE3000

4. If an ISO 27001/ISO 27701 or ISAE 3402 auditor's report is requested, this shall be at the expense of the Data Controller.
5. The certificate shall be provided to the Data Controller without undue delay for its information, via the Processors Trust Center. 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.
6. 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.

Physical Inspection

7. The Data Controller or its representative shall be entitled to carry out inspections of the physical facilities and systems from which the Data Processor processes Personal Data. Physical inspections may, however, only take place at the Data Processor's business premises.
8. To request an inspection, the Data Controller shall submit a detailed inspection plan to the Data Processor no later than **thirty (30) calendar days** prior to the proposed inspection date, describing the proposed scope, duration, and starting time of the inspection.
9. The Data Controller accepts to bear all costs associated with such inspections and agrees that:
10. 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.
11. 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.
12. The Data Processor shall furthermore be entitled to have the Data Controller cover any external costs incurred 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.
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

1. Any other subjects shall be governed by the Main Agreement between the Parties.

CHANGE LOG

VERSION	DATE	INITIALS	CHANGES
1.0	01-05-2025	SK	Published
1.025	01-08-2028	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