Assurance report

Intect ApS

Independent auditor's ISAE 3000 type 1 assurance report with limited assurance on information security and measures pursuant to the data processing agreement with customers who have used the delivery of payroll systems as per 30 April 2025

May 2025

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Disclaimer:

The English version of this report was translated from Danish for the convenience of the reader. This translation has not been reviewed or approved by Grant Thornton's auditors. In all legal matters, please refer to the Danish version.

Section 1: Intect ApS' statement

The accompanying description has been prepared for Intect ApS' customers, who has entered a data processing agreement with Intect ApS and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereinafter "the Regulation") have been complied with.

Intect ApS uses the following sub-processors: Microsoft, Zendesk and JetBrains. This statement does not include control objectives and related controls at Intect ApS' sub-processors. Certain control objectives can only be achieved, if the sub-processor's controls, which are assumed in the design of our controls, are appropriately designed and operationally efficient. The description does not include control activities performed by the sub-processor.

Some of the control objectives stated in Intect ApS' description in Section 3 of the delivery of payroll systems, can only be achieved if the complementary user entity controls (CUEC) with the data controllers have been appropriately designed and works efficiently with the controls with Intect ApS. The report does not include the appropriateness of the design and operating efficiency of these complementary user entity controls.

Intect ApS confirms that:

a) The accompanying description, Section 3, fairly presents how Intect ApS has processed personal data on behalf of data controllers as per 30 April 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Intect ApS' processes and controls related to data protection were designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
   - The procedures used to ensure that the performed data processing has taken place in accordance with contract, instructions, or agreement with the data controller
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
   - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
   - Controls that we, in reference to the scope of Intect ApS have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Does not omit or distort information relevant to the scope of the Intect ApS platform being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect the delivery of payroll systems that the individual data controllers might consider important in their particular circumstances.

b) The controls, related to the control objectives stated in the accompanying description were, in our opinion, suitably designed and implemented as per 30 April 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the General Data Protection Regulation.

Herlev, 5 May 2025
Intect ApS

Frants E. Moraitis
CEO

Section 2: Independent auditor's assurance report with limited assurance on information security and measures pursuant to data processing agreements with data controllers as per 30 April 2025

To Intect ApS, their customers in the role of data controller and their auditors.

Scope

We were engaged to provide assurance about a) Intect ApS' delivery of payroll systems in accordance with the data processing agreement with data controllers as per 30 April 2025 and b) about the design and implementation of controls related to the control objectives stated in the Description.

Intect ApS uses the following sub-processors Microsoft, Zendesk and JetBrains. This statement does not include control objectives and related controls at Intect ApS' sub-processors. Certain control objectives in the description, can only be achieved, if the sub-processor's controls, which are assumed in the design of Intect ApS' controls, are appropriately designed and operationally efficient. The description does not include control activities performed by sub-processors.

Some of the control objectives stated in Intect ApS' description in Section 3 of the delivery of payroll systems, can only be achieved if the complementary user identity controls with the data controllers have been appropriately designed and works effectively with the controls with Intect ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Our opinion is based on limited assurance.

Intect ApS' responsibilities

Intect ApS is responsible for preparing the description and the accompanying statement, Section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Intect ApS' Description and on the design and implementation of controls related to the control objectives stated in that Description, based on our procedures.

We have conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and implemented.

An assurance engagement to report on the Description, design, and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of

its delivery of payroll systems and about the design and implementation of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or implemented. Our procedures did by analysis and inquiries include assessing the implementation of such controls, that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

The scope of the actions we have taken, is less than the ones of an assurance report with reasonable assurance. Hence, the degree of certainty of our opinion is significantly less than the certainty that would have been accomplished, if the assurance report has been issued with a reasonable assurance.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a data processor

Intect ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Intect ApS' payroll systems that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, due to their nature, controls at a data processor may not prevent or detect all breaches of personal data security. Additionally, the projection of any assessment of functionality for future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement Section. During the audit work, we have not found any material aspects, which would lead us to form the opinion:

(a) that the Description does not fairly present Intect ApS' delivery of payroll systems, as designed and implemented as per 30 April 2025, and

(b) that the controls related to the control objectives stated in the Description, not in all aspects were appropriately designed and implemented as per 30 April 2025

Description of assessments of controls

The specific controls, (by analysis and requests) and the nature, timing, and results of those assessments are listed in Section 4.

Intended users and purpose

This report and the description of assessments of controls in Section 4 are intended only for data controllers who have used Intect ApS' platform, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Herlev, 5 May 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Section 3: Intect ApS' description of processing activity for the delivery of payroll systems

The purpose of this description is to provide information to Intect's customers and their stakeholders (including auditors) regarding compliance with the data processing agreements with customers.

Additionally, this description aims to provide information on processing security, technical and organisational measures, and the responsibilities between data controllers (our customers) and Intect.

Intect is a Danish company founded in 2015 and became part of the Norwegian-owned ECIT Group in 2019, which was established in 2013. The company employs approximately 30 people and has its headquarters in Herlev.

Intect offers a wide range of People Management solutions (applications). The service includes operations, support, and consulting. The applications are continuously developed, including functionality updates to comply with applicable laws and regulations. All our applications are developed, operated, and managed by skilled employees in Europe in cooperation with our colleagues in ECIT. ECIT has employees in Sweden, Norway, and Denmark.

The product scope of this description covers the following SaaS solution:

- **Intect Payroll**

Intect develops and operates a payroll system as a Software-as-a-Service (SaaS) application. The application is made available to customers via the internet and is used by small, medium, and large businesses, primarily in the private sector.

Use of the application is by the data controller (the customer) directly through self-service (i.e., via a user ID and password), which means the data processor does not independently perform data processing on the application. Intect also offers additional optional modules that the data controller can choose to include in their subscription for an additional fee.

The scope of this description includes an overview of the technical and organisational security measures implemented in connection with Intect Payroll to protect personal data.

Nature of processing

Intect processes personal data on behalf of the data controller as part of delivering our SaaS solution.

The processing mainly involves the collection, registration, storage, updating, and deletion of personal data necessary for correct payroll processing and compliance with applicable laws.

The purpose of the processing is to support the data controller's payroll administration, including salary calculation, reporting to public authorities, handling absence, vacation, pension, and other HR and employment-related matters.

Intect collects, stores, analyses, and uses personal data about both the data controller and their clients to issue invoices, receive payment information from intermediaries, and disclose relevant data to the data controller.

Personal data

The types of personal data processed through the application depend on each customer and end user's usage.

Processing of special categories of personal data, as per Article 9 of the GDPR, is only carried out if the customer or end user independently chooses to input such information in the application, which occurs under the customer's full responsibility and control. The application is not designed or intended for processing such categories, though users may enter such information in free-text fields.

The processing may include:

- Regular personal data such as identification details (e.g., name, email, phone number, job title)
- Special categories of data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for unique identification, health data, sex life or sexual orientation
- Other sensitive information including criminal data and civil registration numbers
- User activity data, such as IP addresses and audit logs

Categories of data subjects covered by the data processing agreement include:

- The data controller's customers (if considered a natural person)
- Employees of the data controller's customers
- The data controller (if considered a natural person)
- The data controller's employees

Instructions from the data controller

Intect processes personal data according to the instructions from the data controller (customer), as outlined in the data processing agreement and specific terms for using the application.

To ensure compliance:

- All processing activities are limited to the purposes and terms described in the data processing agreement.
- Changes to processing are made based on instructions.
- Employees with access to personal data are instructed that any deviation from the customer's instruction is unacceptable and must be reported.

If Intect deems a customer's instruction to be contrary to the GDPR or other applicable laws:

- Intect will contact the customer as soon as possible for clarification.
- Provide a reasoned explanation of why the instruction is considered illegal.
- Await clarification from the data controller before proceeding with any processing based on that instruction.

Risk assessment

Ongoing risk assessments are conducted regarding the processing of personal data, including likelihood and consequences. These are updated upon significant changes in processing or infrastructure.

The process includes:

- Mapping processing activities and types of data
- Identifying potential threats (e.g., data breaches, unauthorized access, system failure)
- Assessing existing technical and organisational safeguards
- Calculating risk level based on likelihood and impact
- Reviewing after business process or vendor changes

Technical measures

Intect has implemented technical measures deemed relevant for protecting personal data on behalf of the data controller, including:

- IT security policy
- Information security guidelines
- Asset control, including issuance/return during hiring and termination
- Restricted access to personal data for authorized employees
- Cryptography
- Multi-factor authentication
- Vendor relationships and subprocessors oversight
- Incident response and breach handling
- Striving to enter into data processing agreements with subprocessors
- Ensuring equivalent obligations are imposed on subprocessors
- Regular review of risk assessments, policies, and procedures
- Access control based on business needs

These are regularly evaluated and adjusted to meet evolving business and data protection needs.

Organisational measures

Organisational safeguards include:

- Data protection and information security policies shared with all staff
- Access control based on need-to-know and periodic reviews
- Audit logging of system access and actions
- Structured procedures for onboarding and offboarding
- Confidentiality clauses in employment contracts
- Ongoing GDPR training for staff

These are reviewed and adjusted regularly.

Data protection officer (DPO)

Intect has appointed a DPO. Contact details are available to customers and data subjects.

Return and deletion of data

Intect may only delete or return personal data per the terms of the data processing agreement.

Intect has established procedures that ensure the data controller's data is returned or deleted in accordance with the data controller's instructions as specified in the data processing agreement and in accordance with Intect's policies regarding requests from the data controller or termination of cooperation.

Evaluations and deletion routines are regularly reviewed and updated.

Data storage

We strive to ensure that the storage of personal data takes place at the best possible locations, which meet the necessary requirements to protect the information in a responsible and efficient manner, with respect for business operations.

Our processes, which ensure that the information is stored in secure and suitable locations, are continuously assessed to adapt to changes in both legislation and technological conditions

Use of sub-processors

Intect may use sub-processors as part of service delivery, with procedures for:

- **Data processing agreements**: Efforts are made to enter into appropriate data processing agreements with sub-processors, that address relevant requitements in the GDPR and any contractual obligations towards the data controller
- **Requirements for sub-processors**: It is aimed to ensure that significant requirements for the processing of personal data are passed on to sub-processors to an appropriate extent.
- **Notification and Objection**: Data controllers are generally informed about significant changes or replacement of sub-processors, and the opportunity to raise objections is provided.

Sub-processor relationships are regularly reviewed.

Transfers to third countries

Intect strives to ensure that personal data is processed and stored within the EU/EEA in accordance with applicable data protection legislation. We have established internal controls that support the transfer of personal data to secure and approved locations within the EU/EEA.

As a general rule, the transfer of personal data outside the EU/EEA does not occur. In certain cases, personal data may be transferred to Greenland, but only in relation to the processing of information about Greenlandic companies and in accordance with the data controller's instructions. Sub-processors in Greenland are only involved in the processing of data for Greenlandic companies and comply with relevant data protection requirements for the applicable processing.

Data subjects' rights

Intect continuously works to ensure that the rights of data subjects under data protection legislation can be fulfilled in an effective and timely manner. We have established procedures that allow for receiving and processing requests from data subjects, such as requests for access, rectification, deletion, or restriction of personal data.

In the event of requests from data subjects, we offer assistance to the data controllers to ensure proper handling. We support the data controller in assessing and responding to such requests and work to ensure that all necessary steps are taken.

Requests are handled in accordance with the instructions we receive from the data controller, and we adapt our processes to accommodate changes in legislation or business needs

Personal data breaches

Intect has established a series of procedures and controls that help identify any personal data security breaches. This includes, among other things, ongoing awareness campaigns, system monitoring, and log reviews.

When a security breach is identified that may impact the data controller, we strive to notify the data controller as quickly as possible, depending on the nature and complexity of the incident. We work closely with the data controller to ensure that appropriate measures are taken and that the breach is handled correctly.

Our processes for handling security breaches are continuously evaluated to ensure that they are effective and can adapt to changing risks and threat landscapes

Record of processing activities (ROPA)

Intect ensures that our record of data processing is kept up to date to reflect the processing activities we perform on behalf of the data controllers. We include relevant information about both the data controllers and any contact persons, including data protection officers, when applicable.

The record also contains a description of the processing activities carried out, as well as any transfers of personal data to third countries or international organisations, if applicable. If such transfers occur, we ensure that the necessary safeguards are documented in accordance with applicable legislation.

We also describe the overall technical and organisational security measures we have implemented, and we continuously review the record to ensure that it is relevant and up to date with respect to our activities and practices.

Please refer to Section 4, where the specific control activities are described.

Complementary user entity controls at the data controller

Since Intect functions as a data processor, correct and secure processing presupposes that the data controller:

- Ensures that personal data is up to date,
- Ensures that the instructions are legal in relation to the applicable data protection regulations at any given time,
- Ensures that the instructions are appropriate in relation to this data processing agreement and the main service,
- Ensures that the necessary legal basis for processing is present,
- Complies with the obligation to inform data subjects about the exercise of their rights,
- Verifies the identity of data subjects who wish to exercise their rights,
- Configures access rights correctly in the application, including ensuring that the data controller's users are up to date,
- Informs Intect of special requirements or processing activities,
- Provides a legal basis for processing and informs the data subjects,
- Monitors their own use of the application in accordance with the law,
- Uses the application for lawful purposes.

Section 4: Control objectives, control activities, assessment, and results hereof

We have conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our assessment of the implementation has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our assessment has included the controls; we find necessary to establish limited assurance for compliance with the articles stated as per 30 April 2025.

This statement does not include control objectives and accompanying controls with Intect ApS' sub-processor.

Further, controls performed at the data controller are not included in this statement.

We performed our assessment of controls at Intect ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Intect ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that procedures are updated and which updates, if any, have been made. We have inspected list of written procedures, and we have assessed, whether this appears updated and adequate in relation with the scope of the data processing.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected how management ensures that the processing of personal data is only processed according to instructions, and we have assessed the appropriateness of this. We have inspected documentation that the management has assessed that the data processing is being complied with by the data processor and sub-processors	No deviations noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have inspected that there are formalised procedures in place to ensure control that the processing of personal data is not contrary to the General Data Protection Regulation or other legislation. We have inspected that there are formalised procedures for notifying the data controller in cases where the processing of personal data is assessed to be contrary to the law. We have assessed whether it is likely that the data controller will be notified if the instructions, in the data processor's opinion, are contrary to the General Data Protection Regulation or data protection provisions in other EU law or the national law of member states.	We have been informed that the data processor has not received instructions that, in the data processor's opinion, are contrary to the General Data Protection Regulation or data protection provisions in other EU law or the national law of member states. No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that there are formalised procedures in place to ensure that the agreed security measures are established. We have inspected that the procedures are updated, and what updates have been made, if any. We have inspected the overview of written procedures and assessed whether it appears to be updated and sufficient in relation to the agreed security measures.	No deviations noted.
B.2	The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have inspected that there are formalized procedures in place to ensure that the data processor conducts a risk assessment to achieve appropriate security. We have inspected that the conducted risk assessment is updated and covers the current processing of personal data. We have inspected that the data processor has implemented technical measures and how these ensure appropriate security in accordance with the risk assessment	No deviations noted.
B.3	For the PC's used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inquired into whether antivirus software has been installed on the PC's used in the processing of personal data. We have inspected documentation that antivirus software has been installed and updated on a PC.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that external access to systems and databases, used for personal data processing, only takes place through a firewall.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inspected whether internal networks have been segmented to ensure restricted access to systems and databases, used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related needs. We have inspected that users' accesses to systems and databases are restricted to a work-related need.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that systems and databases, used for personal data processing, are monitored, and equipped with alarms.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that technological encryption solutions have been available and active throughout the assurance period. We have, by sample test, inspected that encryption is applied when transmitting confidential and sensitive personal data.	

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inquired into whether policies have been established for setting up the logging of user activities in systems, databases and networks used for personal data processing, including review and follow-up on logs. We have inspected that logging of user activities in systems, databases, and networks, used for personal data processing have been configured and activated. We have inspected that gathered data about user activities in logs are protected against manipulation and deletion.	No deviations noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	We have inquired into whether formalised procedures exist for the use of personal data for development, testing, and similar purposes, ensuring that such use occurs only in pseudonymised or anonymised form. We have, for a randomly selected development and test database, inspected that the personal data contained therein are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in penetration tests.	We have inquired whether formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. We have inspected that documentation exists regarding regular testing of the technical measures established. We have inquired into whether deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inquired into whether formalised procedures exist for handling changes to systems, databases, and networks, including handling of relevant updates, patches, and security patches. We have, by extracting or reviewing technical security parameters and configurations for a single instance of each type of systems, databases, and networks in use, inspected that these are updated with agreed changes and relevant updates, patches, and security patches.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' rights are assessed on a regular basis, including that rights are still based on a work-related need.	We have inquired whether formalised procedures exist for granting and revoking user access to systems and databases used for processing personal data. We have, for a single employee from each group of employees, inspected that access to systems and databases is approved and based on a work-related need. We have, for a single randomly selected former employee, inspected that their access to systems and databases has been deactivated or terminated in a timely manner. We have inspected documentation to ensure that periodic review and approval of assigned user access have been carried out as planned.	No deviations noted.
B.14	Access to systems and databases processing personal data that involve a high risk for the data subjects are as a minimum only accessed by using two-factor authentication.	We have inquired into whether formalised procedures exist, ensuring that two-factor authentication is used when processing personal data involving a high risk for the data subjects. We have inspected that developers' users' access to processing personal data involving high risk for the data subjects, only take place by using two-factor authentication.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inquired whether formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. We have, for randomly selected premises and data centres, where personal data are stored and processed, inspected that it is likely that only authorised individuals have physical access to these locations.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists, that management has assessed and approved within the past year. We have inquired into whether the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inquired about management's assessment of whether the information security policy generally complies with the requirements for security measures and processing security outlined in the signed data processing agreements. We have, through a representative data processing agreement, inspected that the requirements in the agreements are covered by the information security policy's requirements for security measures and processing security.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inquired into whether formalised procedures exist to ensure that the data processor's employees are screened as part of the employment process. We have inquired whether the most recently hired employee has been subjected to screening during the hiring process.	We have not received documentation confirming that the most recently hired employee was subjected to screening during the hiring process. However, we have been informed that the most recently hired employee was transferred from a sister company and joined Intect without undergoing screening. No further deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have, for the most recently hired employee, inspected that the employee in question has signed a confidentiality agreement.	No deviations noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inspected that procedures exist to ensure that terminated employees' rights are inactivated or deleted upon resignation, and that assets such as access cards, computers, mobile phones etcetera are returned. We have, for the most recently terminated employee, inspected that access rights have been deactivated or terminated and that assets have been returned.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the non-disclosure agreement and the general duty of confidentiality. We have, for the most recently terminated employee, inspected that documentation exist of the continued validity of the non-disclosure agreement and the general duty of confidentiality.	No deviations noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have inquired into whether the data processor provides awareness training for the employees, including general IT-security and GDPR. We have inspected documentation that all employees who either have access to or process personal information, have completed the provided awareness training.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inspected, whether the company has assessed the need for a DPO.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
C.9	The processor keeps a record of categories of processing activities for each data controller. Management has ensured that the record of categories of processing activities for each controller includes: • Name and contact information of the data processor, the data controller, representatives of the data controller and data protection officers • The categories of processing, carried out on behalf of the individual data controller. • When relevant, information about transfer to third countries or an international organisation, with documentation of adequate guarantees. • Where possible, a general description of technical and organisational security measures. Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inspected that the list has been assessed and approved by management within the last year. We have inspected that the list includes: • Name and contact information of the data processor, the data controller, representatives of the data controller and data protection officers • The categories of processing, carried out on behalf of the individual data controller. • When relevant, information about transfer to third countries or an international organisation, with documentation of adequate guarantees. • Where possible, a general description of technical and organisational security measures.	No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for the storage and deletion of personal data in accordance with the agreement with the data controller. We have inspected that the procedures are updated, and which updates have been made, if any. We have inspected the list of written procedures and assessed whether this appears to be updated and adequate in relation to the agreed storage and deletion of personal data.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storing, and deletion contains the specific requirements for the data processor's storage periods and deletion routines. We have, for a randomly selected data processing activity from the data processor's list of processing activities, inspected that there is documentation confirming that personal data are stored in accordance with agreed storage periods and deletion routines.	No deviations noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formal procedures are in place for processing the data controller's data upon termination of the processing of personal data. We have inquired into whether there have been any discontinued processing activities within the last six months.	We have been informed that there have been no discontinued processing activities of personal data within the past six months. No deviations noted

Control objective E – Storage of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures or policies exist that storage and processing of personal data are only performed in accordance with the data processing agreements. We have inquired into whether the procedures have been assessed on a regular basis.	No deviations noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have inspected that the data processor maintains a comprehensive and updated overview of processing activities, including the specification of locations, countries, or regions. We have inspected that there is documentation confirming that data processing, including the storage of personal data, is conducted solely at the locations specified in the data processing agreement—or otherwise approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are being updated, and which updates have been performed.	No deviations noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-processors used and approved by the data controllers.	No deviations noted.
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller.	We have inspected that formalised procedures are in place for informing the data controller upon changes in the sub-processors used. We have inspected that the data controllers have been informed about changes in the approved sub-processors used.	No deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inquired whether signed sub-processor agreements exist with the sub-processors listed in the data processor's overview. We have, for a randomly selected sub-processor agreement, inspected that it contains the same requirements and obligations as those outlined in the data processing agreement between the data controllers and the data processor.	No deviations noted.
F.5	The data processor has a list of approved sub-processors.	We have inspected that the data processor has a complete and updated list of sub-processors used and approved.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor.	We have inspected documentation confirming that a risk assessment has been conducted for sub-processors and the current processing activity at their location, as well as that planned follow-up actions have been carried out in accordance with the risk assessment. We have inspected documentation confirming that supervision has been conducted for sub-processors listed in the data processing agreements with the data controllers.	No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures exist to ensure that personal data are transferred to third countries or international organisations only in accordance with the agreement with the data controller and based on a valid basis of transfer. We have inquired about when the procedures were last updated and reviewed, and which updates that may have been made. We have inspected the overview of written procedures and assessed whether it appears to be updated and adequate in relation to the transfer of personal data	No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inquired whether the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. We have inspected, for a randomly selected data transfer from the data processor's overview of transfers, that there is a requirement for the data processor to transfer personal data only based on instructions from the data controller.	We have been informed, that personal data are not being transferred to third countries or international organisations. No deviations noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	We have inquired into whether formalised procedures are in place for ensuring a valid basis of transfer. We have inquired about when procedures have been updated, and which updates have been made, if any. We have, for a randomly selected data transfer from the data processor's overview of transfers, inspected that there is documentation for a valid transfer basis in the data processing agreement with the data controller, and that transfers have only occurred to the extent agreed with the data controller.	We have been informed, that personal data are not being transferred to third countries or international organisations. No deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are updated and if so, which updates have been made. We have inspected the overview of written procedures and assessed whether they appear updated and adequate in relation to assistance to the data controller.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have inspected that the procedure for assistance to the data controller includes detailed procedures for: • Return of personal data • Correction of personal data • Deletion of personal data • Restriction of processing of personal data • Information about processing of personal data to the data subject We have assessed whether it is likely that the systems and databases in use, support the implementation of the mentioned detailed procedures	We have been informed, that the data processor has not received any requests from the data controller in relation to the data subjects' rights. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inquired into whether procedures are updated and which updates, if any, have been performed. We have inspected list of written procedures and assessed whether these appear to be updated and adequate in relation to the managing of personal data breaches.	No deviations noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic Follow-up on logging of access to personal data.	We have inspected that the data processor offers awarenesstraining to the employees, related to identifying possible personal data breaches. We have inspected documentation, that network traffic is monitored and that abnormalities and alarms are being followed up on. We have inspected that logging of systems has been implemented and that follow-up on activities is conducted accordingly.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.	We have inquired into whether the data processor has an overview of security incidents, disclosing whether the individual incidents involved a personal data breach. We have inquired into whether the data processor has included possible personal data breaches at the sub-processor, in the data processor's list of personal data security breaches. We have inquired into whether all recorded personal data breaches at the data processor or sub-processors have been reported to the affected data controllers without undue delay after the data processor became aware of the personal data breach.	We have been informed, that the data processor has not received any requests from the data controller in relation to the data subjects' rights. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No	*Intect ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. • The nature of the personal data breach • Probable consequences of the personal data breach • Measures, taken or proposed to be taken to respond to the personal data breach.	We have inquired whether the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have assessed whether it is likely that procedures exist to support that measures are taken to manage the personal data breach.	We have been informed, that the data processor has not received any requests from the data controller in relation to the data subjects' rights. No deviations noted.