Standard Contractual Clause

Companies which have a:

Cooperation agreement/customer contract

(Hereafter the “data controller”)

And

IntraManager A/S

CVR 33966458

Helgavej 26

Denmark

(Hereafter the “data processor”)

Each a “party”; together “the parties”

HAVE AGREED on the following Contractual Clauses (the Clauses) for the purpose of complying with the Data Protection Regulation and secure the protection of privacy and physical beings fundamental rights and freedom rights.

1. Table of Contents

2 Background for the Standard Contractual Clauses

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.

2. Designed to ensure the parties compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), which sets up specific demands to the content of a Standard Contractual Clause.

3. The data processor will process personal data on behalf of the data controller in accordance with "The main agreement".

4. The Clauses and the "main agreement" are mutually dependent and cannot be terminated separately. However, the Clauses can – without terminating the "main agreement" – be replaced by another valid Clause.

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

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

7. Appendix A contains details about the processing, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

8. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.

9. 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.

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

11. Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3 The rights and obligations of the data controller

1. The data controller is by default responsible to the outside world (including the registered) for ensuring that the processing of personal data takes place in compliance with the GDPR and the Data Protection Act.

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

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

4 The data processor acts according to instructions

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 data processor is subject to. If so, the data processor shall inform the data controller about the legal demand prior to processing unless that law prohibits such information on important grounds of public interest, see Article 28(3) litra a.

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

5 Confidentiality

1. The data processor ensures that only persons who are currently authorized hereto have access to the personal data that are processed by the data controller. The access to information must be shut down immediately if the authorization is withdrawn or expires.

2. Authorization can only be given to persons to whom it is necessary to have access to personal data to fulfill the data processors' obligations towards the data controller.

3. The data processor ensures that persons who are authorized to process personal information on behalf of the data controller has committed to confidentiality or are subjected to an adequate statutory confidentiality.

4. The data processor shall at the request of the data controller, demonstrate that the relevant persons under the data processor’s authority are subject to the abovementioned confidentiality.

6 Security of processing

1. The data processor shall implement all measures required by Article 32 of the GDPR of which it is evident that taking account of the current level, implementation costs and the character of the processing in question, proportion, context, and purpose as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of protection appropriate to the risks.

2. The above-mentioned obligation signifies that the data processor shall conduct an evaluation of risks and subsequently implement measures to mitigate the identified risks. Depending on their relevance, the measures may include the following:

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

3. In connection with the above-mentioned, the data processor shall in all cases as a minimum implement the level of security and the measures which are specified in more detail in Appendix C.

4. The parties' possible regulation/agreement upon remuneration or similar in connection to the data controller or the data processors subsequent demands about establishing of further safety measures will be evident in the parties "main agreement".

7 Use of sub-processors

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

2. The detailed conditions towards the data processor's use of possible sub-processors can be seen in Appendix B.

3. When the data processor has informed the data controller to make use of a sub-processor and has updated Appendix B, the data processor has ensured to impose the sub-processor the same data protection obligations as those which has been set in the Clause through a contract or other legal document under Union or Member State law, providing in particular the necessary guarantees that the sub-processor will implement the appropriate technical and organizational measures in such a way that the processing complies with the GDPR.

   The data processor is therefore responsible for the conclusion of a sub-processor agreement to impose a potential sub-processor at least those obligations which the data processor is obliged to hence the data protection rules and the Clauses with additional Appendices.

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business-related issues (such as prices) that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g., enabling the data controller to instruct the sub-processor to delete or return the personal data.

6. If the sub-processor does not fulfill his data protection obligations, the data processor shall remain fully liable to the data controller in regard to the fulfillment of the obligations of the sub-processor.

8 Transfer data to third countries or international organizations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur based on documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organizations, 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 to, 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 interests.

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. process personal data in a third country

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

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

9 Assistance to the data controller

1. Considering the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of the data controller's obligations to respond to requests for exercising the data subjects' rights laid down in Chapter III GDPR.

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

    a. the right to be informed when collecting personal data from the data subject
    b. the right to be informed when personal data have not been obtained from the data subject
    c. the right of access by the data subject
    d. the right to rectification
    e. the right to erasure ('the right to be forgotten')
    f. the right to restriction of processing

g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. The data processor shall assist the data controller in securing compliance of the data responsible obligations pursuant to the GDPR Article 32-36 considering the nature of the processing and the information available to the data processor, see Article 28(3) litra f.

   This entail that the data controller, in regard of the character of the processed, shall assist the data responsible in connection to ensure the data responsible comply with:

   a. The data controller´s obligation to carry out appropriate technical and organizational measures to ensure a level of security that is appropriate to the risks that relate to the processing.
   b. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority (The Danish Data Protection Agency), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
   c. 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.
   d. The data controller's obligation to carry out a data protection impact assessment regarding data protection if a type of processing is likely to carry a high risk to the rights and freedoms of natural persons.
   e. The data controller's obligation to consult the competent supervisory authority, 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.

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

10 Notification of personal data breach

1. In case of any personal data breach at the data processor or sub-processor, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority within 72 hours.

3. In accordance with Clause 9(2)(b), the data processor – considering the character of the process and the information available - 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 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.

11 Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor is obliged, at the option of the data controller, to delete or return all personal data, as well as deleting existing copies unless Union or Member State law requires storage of the personal data.

12 Audit and inspection

1. The data processor shall make all information available to the data controller necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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

13 The parties' agreement on other terms

1. A possible (special) regulation of the parties' violation of the clauses will appear in the parties "main agreement".

2. A possible regulation of other conditions between the parties will appear in the parties "main agreement".

14 Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature on the "main agreement" and where no other Clause has been made.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The parties' possible regulation/agreement of remuneration, conditions, and the like in connection to changes of the Clauses will appear in the parties' "main agreement".

4. Termination of the Clauses may be effected in accordance with the termination conditions inclusive term of notice which appears in the "main agreement"

5. The Clauses shall apply for the duration of the provision of the processing services. No matter the "main agreement" and/or the data processor's termination, the Clauses will still apply until the processing ceases and the information has been deleted by the data processor and possible sub-processors.

15 Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points which are mentioned in the parties' "main agreement".

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

16 Signature

On behalf of the data processor:

Date	10th of June 2023
Name	Lars Klausen
Position	CEO
Phone number	+45 33 60 66 09
E-mail	lk@intramanager.com

Signature _____

Appendix A Information about the processing

The purpose of the data processor's processing of personal data on behalf of the data controller is:
That the data controller can use the systems "IntraManager Work" and "IntraManager Board" which are owned and managed by the data processor to collect and process information about the data controllers' customers and/or employees.

The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
That the data processor provides the systems "IntraManager Work" and "IntraManager Board" to the data controller and thereby stores personal information about the data controller's customers and/or employees on the company's servers.

The processing includes the following types of personal data about data subjects:
Name, e-mail address, telephone number, address, social security number, employee number, customer number, bank information, product information.

Processing includes the following categories of the registered:
Employees and customers (current and potential customers)

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:
The processing is non-fixed-term and lasts until the agreement is terminated by one of the parties.

Appendix B Sub-processors

B.1 Authorized sub-processors

On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

Company	Amazon Web Services EMEA SARL (AWS Europe)
Registration no.	B 186284
Address	38 Avenue John F. Kennedy L-1855 Luxembourg
Processing	Specific Data center hosting of servers
Data location	Greenhills Road, Tymon North, Dublin Ireland
Specific	AWS is used for hosting the solution, including storage and processing of data, all data is processed in the platform, including customers' personal data. Data is stored encrypted. This processing of data is contractually obliged by AWS to carry out within the EU-WEST (Ireland) data region, and thus within the EU / EEA. The supplier does NOT make use of a support agreement at AWS since this does not have the same protection. A TIA is devised yearly (Transfer Impact Assessment)

Company	Zendesk International Ltd.
Registration no.	519184
Address	1019 Market Street San Francisco U.S.A.
Processing	Support tickets
Specific	Zendesk is an American registered company that stores data outside the EU. Since they are to be found on the "Privacy Shield" list and has issued a Standard Contractual Clause for use, we are free to use them as a supplier and for storage of the customer´s email-addresses and names. A TIA is devised yearly (Transfer Impact Assessment)

Company	inMobile ApS
Registration no.	DK31426472
Address	Axel Kiers Vej 18 L
	8270 Højbjerg
	Denmark
Processing	SMS Gateway
Specific	This sub-processor is exclusively used if the data controller chooses to make use of the data processor's service for system SMS.

Company	Criipto ApS
Registration no.	DK35142207
Address	Dronninggårds Alle 136
	2840 Holte
	Denmark
Processing	MitID broker
Specific	This sub-processor is exclusively used if the data controller makes use of the data processors service for digital signing with MitID.

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

Appendix C Instruction pertaining to the use of personal data

C.1 The subject of/instruction of processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following: General operations, including hosting, viewing, organizing, receiving, retrieving, forwarding, structuring, customizing, deploying, searching, processing, storing, restoring, deleting, limiting, maintaining, developing, modeling, logging, support, debugging and other IT services related to the data processor's delivery of the software platform to the data controller in accordance with the subscription agreement entered between the parties for the data processor's software solution.

C.2 Security of processing

Since the data processor's software enables the data controller to upload and otherwise add data to the platform, the data processor will potentially process an unknown amount of personal data and unknown categories of personal data and data subjects. Therefore, the data processor has chosen to implement a general level of security reflecting that a larger amount of personal data and all kinds of categories of personal data and data subjects may be processed.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Information security

The data processor has implemented policies, controls and processes that covers the information security areas described below:

Confidentiality: Ensure that unauthorized persons cannot access data that could be misused to the detriment of the data processor's customers, business associates and employees.

Integrity: Ensure that systems contain accurate and complete information.

Availability: Ensure that relevant information and relevant systems are accessible and stable.

Instructions

There are written procedures which require that personal data may only be processed when an instruction is available. An assessment is made on an ongoing basis - and at least once a year - of whether the procedures need to be updated. The data processor only performs the processing of personal data, which appears from instructions from the data controller.

Physical security

The data processor shall maintain physical security measures to secure sites used for the processing of personal data, including the storage of personal data covered by the Clauses against unauthorized access and tampering.

The data controller shall have appropriate technical measures in place to limit the risk of any unauthorized access to premises where personal data is processed. In addition, the data controller shall, where necessary, evaluate and improve the effectiveness of such measures. Ensure that the level of physical security at all times is in line with the current threat landscape and the sensitivity and amount of personal data covered by the Clauses.

Communication connections and encryption

The data processor has appropriate technical measures to protect systems and networks, including the protection of data during transmission and access via the Internet, as well as to limit the risk of unauthorized access and/or installation of malicious code.

The data processor uses appropriate encryption technologies and other equivalent measures in accordance with the requirements of the law, approved standards for encryption of classified information as well as good data processing practice.

To the extent required by applicable national and international law, standards for encryption of classified information or good data processing practices, the data processor shall use encryption technologies and other equivalent measures.

Transmission of sensitive and confidential information over the Internet is protected by encryption. Technological solutions for encryption are available and activated. Firewall only allows encrypted data traffic. Formalized procedures are in place to ensure that the transmission of sensitive and confidential information over the Internet is protected by strong encryption based on a recognized algorithm.

Encryption keys are managed on behalf of the data controller and under the control of the data processor, so that sub-processors or others do not have access to the customer's data in clear text. The data processor is obligated to encrypt data which is processed on behalf of the data controller in the data processor’s application before transfer of personal information to sub-processors stated in B.1.

Firewall or similar technical measures

External access to systems and databases used for processing personal data is provided through a VPN. Administrative access shall be available to maintain the firewall configuration and ruleset.

Antivirus

The systems and databases used for the processing of personal data have antivirus installed and are regularly updated.

Security backup

The data processor shall have internal contingency procedures in place to ensure the restoration of services without undue delay in the event of downtime under the main agreement. The data processor ensures backup.

Backup of configuration files and data shall take place in an uninterrupted process so that relevant data can be restored. The backups are stored in such a way that they are not accidentally or unlawfully (e.g., by fire, flood, accident, theft, or the like) destroyed, lost, deteriorated, disclosed, misused, or otherwise processed in breach of the rules and regulations applicable at any time to the processing of personal data.

The backups shall be kept physically separate from primary data and in a security approved data center.

The data processor uses a redundant environment to ensure access and continuous operation of the software solution. The data processor ensures that backups are stored in their entirety.

Use of home / remote workplaces

Where data processing is carried out from ad hoc and/or home workplaces, the data processor shall ensure that these comply with the security requirements of these Clauses and its appendices and the law in general.

The data processor shall comply with, inter alia, the following:

- That an encrypted connection is used between the ad hoc workplace and the data processor's/data controller's network.
- The data processor has internal instructions for its own employees regarding ad hoc and home workplaces.

In addition, where technically feasible, the data processor shall use two-factor authentication.

Logging

1. There are formalized procedures for setting up logging user activities in systems, databases and networks used for the processing and transmission of personal data.
2. The data processor ensures that the scope of the security log is defined based on a risk assessment carried out by the data processor.
3. The data processor ensures that there is sufficient space for the security logs to be stored for the period.
4. The data processor ensures that regular spot checks are carried out to ensure that the security logs contain what is expected.
5. The data processor weighs the deletion periods of the security logs between the possibility to analyze cyber-attacks, to support investigations and the protection of the rights and freedoms of natural persons.
6. The data processor ensures that information collected on user activity in logs is protected against deletion and tampering.
7. The data processor ensures that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and enabled.
8. The data processor ensures logging in all environments where personal data are processed.
9. Activities performed by system administrators and others with special rights.
10. Changes to logging settings, including disabling logging.
11. Changes in system rights for users.
12. Failed attempts to log-on to systems, databases, and networks.

User administration

The data processor ensures that the solution supports appropriate user administration. The data controller is ensured the possibility to use automatic or manual user administration.

The solution supports the creation, periodic review, and termination of users. The data controller alone may perform these functions, but the data processor may assist where necessary and within reasonable extent.

Instruction of employees

The data processor ensures that employees are aware of and have adequate training and instruction on the purpose of the data processing, policies, workflows and on their duty of confidentiality.

An information security policy is in place, which has been reviewed and approved by management within the last year. The information security policy has been communicated to relevant stakeholders, including the data processor's employees.

The information security policy in general complies with the requirements on safeguards and security of processing in the Clauses concluded.

Formalized procedures are in place to ensure verification of the data processor’s employees at the time of recruitment.

Employees have signed a confidentiality agreement at the time of employment. Employees have been introduced to:

- Information Security Policy
- Data processing procedures and other relevant information

Procedures are in place to ensure that the rights of departing employees are deactivated or terminated upon resignation, and that assets such as access cards, PCs, mobile phones, etc. are confiscated.

Formalized procedures are in place to ensure that resigning employees are made aware of the maintenance of the confidentiality agreement and the general duty of confidentiality. The contract of employment contains guidelines on the duty of confidentiality of employees after termination of employment.

The data processor provides awareness training to employees covering general IT security and processing security in relation to personal data.

There is evidence that all employees who either access or process personal data have completed the awareness training offered.

The employees of the data processor are obliged to follow internal procedure on the use of support from sub-processors used. The purpose of the procedure is to ensure the correct use of support and to prevent the use of "follow the sun" support, thereby eliminating the risk of personal data being accessed from insecure third countries.

Notification in the exercise of official authority

A procedure has been established for notifying the data controller of any direct or indirect request by the authorities for the supply of or access to data.

Disposal of equipment

The data processor must have formal processes in place to ensure that the effective erasure of personal data takes place prior to the disposal of electronic equipment.

C.3 Assistance to the data controller

The data processor shall, to the extent possible – within the scope and extent set out below – assist the data controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organizational measures.

The data processor will, where possible and where compliance requires the assistance of the data processor, assist the data controller in fulfilling the data controller's obligation to respond to requests for the exercise of data subjects' rights as set out in Chapter III of the Regulation 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.

Given that the data processor processes, in principle, only the general personal data of the data controller's users of the software solution, the data processor has implemented such technical and organizational measures as to allow the immediate export of those users' personal data and will therefore be able to assist the data controller, as well as to freely dispose of the data otherwise provided by the data controller.

In the event of a breach or incident as referred to in section 9.2, the data processor shall provide the following information:

- Facts about the observed breach (time, place, cause)
- When the breach started, when it was detected and when the breach was stopped
- The nature of the personal data breach, including whether there has been a breach of confidentiality, integrity, and availability
- The categories and approximate number of data subjects affected, if possible
- The categories of personal data, if possible
- Name and contact details of contact point where further information can be obtained
- Description of plausible consequences of the breach
- Description of measures taken, or proposed to be taken, to address the breach and its possible adverse effects

C.4 Storage period / erasure procedures

The platform is configured to follow erasure procedures set by the controller.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller’s original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5 Processing location

Processing of the personal data under the Clauses cannot be performed, without prior written consent of the data controller, at locations other than the place of establishment of the data processor or the locations used by the sub-processors referred to in Appendix B.1.

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

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

The data processer may not transfer personal data to or access personal data from other countries outside the EEA or international organizations.

If the data controller successively has received documented written instructions from the data processor, the data controller is obligated to ensure that (i) a such transfer is legal, comprising that a suitable level of protection for the transfer of personal data, with entering of the EU commissions standard contractual agreements or other legal foundation for the transfer shall be stated, (ii) all necessary approvals are gathered, and (iii) all necessary announcements regarding the concerned transfer has been given to the relevant supervisory authority. The data processor is obligated to update the schedule in Appendix B.1 and state the reason for the transfer, cf. in the GDPR chapter V.

C.7 Procedures for the data controller´s audit with the processing which is done by the data processor

The data processor shall at least once a year be available to the data controller for the purpose of the data controller's verification of the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller may, against payment, contest the scope and/or methodology of the report and may, in such cases, request a new audit/inspection under a revised scope and/or different methodology.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the data processor. Such inspections shall be performed when the data controller deems them required and shall be organized in such a way that they are of the least possible inconvenience to the data processor.

The data controller's costs, if applicable, relating to physical and/or written inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection, whether this is physical and/or written.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

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

The data processor shall annually, at its own expense, perform an audit, where the processing of personal data is carried out by the sub-processor, related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's inspection of sub-processors shall be organized in such a way as to ensure adequate insight into and control of the sub-processors' compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The audit may consist of obtaining an audit opinion or inspection report from an independent third party, inspections, and/or written questions. The data processor shall in principle have a free choice as to the method of supervision of sub-processors. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit under a revised scope and/or different methodology.

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

Based on the results of a declaration or of the supervision of sub-processors, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Lars Nicolai Balslev Klausen
CEO
På vegne af: INTRAMANAGER A/S
Serienummer: aa51cf77-b71d-4b3a-b61c-493c5f733273
IP: 87.52.xxx.xxx
2023-06-15 11:52:20 UTC

Mit ID