

Data Processing Agreement Prepared in Accordance with the Standard Contractual Clauses Accepted by the European Data Protection Council

Data Processing Agreement (EU)

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Kunde

-

--

DK

Company registration number:
hereinafter "The Controller"

and

nps.today ApS

Lyngbyvej 16

2100 København

DK

Company registration number: 36464917
hereinafter "The Processor"

each a "Party"; together the "Parties"

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

This is version 8, last updated 03.09.2025 15:13.

Table of contents

1. Preamble.....	3
2. The rights and obligations of the Controller	3
3. The Processor acts according to instructions	4
4. Confidentiality.....	4
5. Security of processing.....	4
6. Use of sub-processors.....	5
7. Transfer of data to third countries or international organisations	6
8. Assistance to The Controller.....	7
9. Notification of personal data breach.....	8
10. Erasure and return of data.....	7
11. Audit and inspection.....	9
12. The parties' agreement on other terms.....	9
13. Commencement and termination.....	9
14. The controller and the processor contacts/contact points	10

Appendix

Appendix A Information about the processing	11
Appendix B Authorised Sub-processors.....	12
Appendix C Instruction pertaining to the use of personal data	13
Appendix D The Parties' terms of agreement on other subjects	18

1. **Preamble**

- 1.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the Controller.
- 1.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).
- 1.3 In the context of the provision of Agreement on the Data Controller's ordering of services and use of the Data Processor's software as defined in the Data Processor's terms and conditions., the Processor will process personal data on behalf of the Controller in accordance with the Clauses.
- 1.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 1.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.
- 1.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- 1.7 Appendix B contains the Controller's conditions for the Processor's use of sub-processors and a list of sub-processors authorised by the Controller.
- 1.8 Appendix C contains the Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Processor and how audits of the Processor and any sub-processors are to be performed.
- 1.9 Appendix D contains provisions for other activities which are not covered by the Clauses.
- 1.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
- 1.11 The Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

2. **The rights and obligations of the Controller**

- 2.1 The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.
- 2.2 The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

- 2.3 The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

3. **The Processor acts according to instructions**

- 3.1 The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
- 3.2 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. **Confidentiality**

- 4.1 The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
- 4.2 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

5. **Security of processing**

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

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

- 5.1.1 Pseudonymisation and encryption of personal data;
- 5.1.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- 5.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - 5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 5.2 According to GDPR, Article 32, the Processor shall also – independently from the Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Controller shall provide the Processor with all information necessary to identify and evaluate such risks.
- 5.3 Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR, Article 32, by inter alia providing the Controller with information concerning the technical and organisational measures already implemented by the Processor pursuant to GDPR, Article 32, along with all other information necessary for the Controller to comply with the Controller's obligation under GDPR, Article 32.

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

6. **Use of sub-processors**

- 6.1 The Processor shall meet the requirements specified in GDPR, Article 28(2) and (4) in order to engage another processor (a sub-processor).
- 6.2 The Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Controller.
- 6.3 The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 60 days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the Controller can be found in Appendix B.
- 6.4 Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and GDPR.

The processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Processor is subject pursuant to the Clauses and GDPR.

- 6.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Controller.
- 6.6 The Processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
- 6.7 If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in GDPR, Articles 79 and 82 – against the Controller and the Processor, including the sub-processor.
- 6.8 Objection Right for new sub-processors.

The Data Controller may object to Data Processors use of a new sub-processor by notifying Data Processor in writing within thirty (30) business days after receipt of nps.today notice by a notification in writing to privacy@npstoday.com. In the event that the Data Controller objects to a new sub-processor, Data Processor will use reasonable efforts to make available to the Data Controller a change in the Services or recommend a commercially reasonable change to Data Controllers configuration or use of the Services to avoid processing of personal data by the objected to new sub-processor without unreasonably burdening the Data Controller. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, the Data Controller may terminate the applicable Agreements with respect to those Services which cannot be provided by Data Processor without the use of the objected to new sub-processor by providing written notice to Data Processor.

7. **Transfer of data to third countries or international organisations**

- 7.1 Any transfer of personal data to third countries or international organisations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.
- 7.2 In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, is required under EU or Member State law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement prior to processing unless that law prohibits such information

on important grounds of public interest.

7.3 Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Clauses:

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

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

7.3.3 have the personal data processed by the Processor in a third country

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

8. **Assistance to The Controller**

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

This entails that the Processor shall, insofar as this is possible, assist the Data Controller in the Controller's compliance with:

8.1.1 the right to be informed when collecting personal data from the data subject

8.1.2 the right to be informed when personal data have not been obtained from the data subject

8.1.3 the right of access by the data subject

8.1.4 the right to rectification

8.1.5 the right to erasure ('the right to be forgotten')

8.1.6 the right to restriction of processing

8.1.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

8.1.8 the right to data portability

8.1.9 the right to object

8.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

- 8.2 In addition to the Processor's obligation to assist the Controller pursuant to Clause [5.3](#), the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:
- 8.2.1 The 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 data protection agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - 8.2.2 The 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;
 - 8.2.3 The Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - 8.2.4 The Controller's obligation to consult the competent data protection agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by The Controller to mitigate the risk.
- 8.3 The Parties shall define in [Appendix C](#) the appropriate technical and organisational measures by which The Processor is required to assist the controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause [8.1](#) and [8.2](#).

9. **Notification of personal data breach**

- 9.1 In case of any personal data breach, the Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach.
- 9.2 The Processor's notification to the Controller shall, if possible, take place within immediately and no later than 12 hours after the processor has become aware of the breach of the personal data security after the Processor has become aware of the personal data breach to enable the Controller to comply with the Controller's obligation to notify the personal data breach to the data protection agency, cf. GDPR, Article 33.
- 9.3 In accordance with Clause [8.2.1](#), the Processor shall assist The Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to GDPR, Article 33(3), shall be stated in the Controller's notification to the competent data protection authority:
- 9.3.1 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;

9.3.2 the likely consequences of the personal data breach;

9.3.3 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.

9.4 The parties shall define in [Appendix D](#) all the elements to be provided by the Processor when assisting the Controller in the notification of a personal data breach to the competent data protection agency.

10. **Erasure and return of data**

10.1 On termination of the provision of personal data processing services, the Processor shall be under obligation to delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so unless Union or Member State law requires storage of the personal data.

11. **Audit and inspection**

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

11.2 Procedures applicable to the Controller's audits, including inspections, of the Processor and sub-processors are specified in [C.7](#) and [C.8](#).

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

12. **The parties' agreement on other terms**

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

13. **Commencement and termination**

- 13.1 The Clauses are binding upon the Parties.
- 13.2 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.
- 13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.
- 13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Controller pursuant to Clause [10.1](#) and Appendix [C.4](#), the Clauses may be terminated by written notice by either Party.
- 13.5 The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence.

14. **The controller and the processor contacts/contact points**

- 14.1 The Parties may contact each other using the following contacts/contact points
- 14.2 The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for The Controller:
Reference is made to the contact information in the main agreement.

Contact information for The Processor:
Reference is made to the contact information in the main agreement.

Appendix A Information about the processing

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

- 1.1 The following purposes form the basis of the Processor's processing of personal data on behalf of the Controller:

The Data Controller may use the nps.today software, which is owned and managed by the Data Processor, to collect and process loyalty information about the Data Controller's customers, partners, members and/or employees.

2. The Processor's processing of personal data on behalf of the Controller shall mainly pertain to (the nature of the processing):

- 2.1 The Data Processor makes the nps.today software available to the Data Controller and thereby stores the personal data that the Data Controller enters and stores in the software. Additionally, the respondents will fill out the distributed survey, which will be sent out by the Data Controller.

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

- 3.1 e-mail, name, phone number, IP-address

NPS Score, NPS comment, customer ID and, timestamp.

4. Processing includes the following categories of data subject

- 4.1 Persons who have or have had a direct or indirect customer and/or employee relationship with the Data Controller. (Survey participants).

5. The Processor's processing of personal data on behalf of the Controller may be performed when the Clauses commence. The processing has the following duration:

- 5.1 The processing of personal data shall be performed until the Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause [11](#). The Processor's processing of personal data is performed as long as the underlying commercial agreement(s) consists.

Appendix B Authorised Sub-processors

1. Approved sub-processors

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

Microsoft Ireland Operations Limited (Data storage and processing) VAT: IE8256796U
Flowmailer (NL) (email delivery) VAT: NL854692538B01
Link Mobility Group (EU) (SMS delivery) VAT: 984 066 910

- 1.2 The Processor has the Controller's general authorisation for the engagement of sub-processor(s) from the above list. The Processor shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 60 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the data exporter to exercise its right to object.

Appendix C Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

- 1.1 The Data Controller may use the nps.today system, which is owned and managed by the Data Processor, to collect and process loyalty information about the Data Controller's customers, partners, members and/or employees.

2. Security of processing

- 2.1 The level of security shall take into account:

Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Processor must implement an appropriate level of security.

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

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

Organizational security

The Processor shall implement the following organizational security measures:

- a) The employee access to personal data is limited, so that only the relevant employees have access to the necessary personal data.
- b) All employees of the Processor are subject to confidentiality obligations that apply to all processing of personal data.
- c) The Processor has established procedures that ensure proper deletion or continuous confidentiality when the hardware is repaired, serviced, or disposed.
- d) The Processor has an IT security policy.
- e) The Processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually.
- f) The processing of personal data done by the employees of the Processor is logged and can be checked as required.
- g) The Processor has the opportunity to respond to employees' breaches of the processor's data security or breach of instructions on the processing of personal data according to employment law.
- h) The Processor's employees regularly document and report breaches of personal data security or risks thereof.

The organization has implemented two-factor authentication as a mandatory requirement for all employees when logging into systems, ensuring an enhanced level of security and data protection.

Technical security: Access to and protection of IT systems

The Processor shall implement the following technical security measures regarding access to and protection of IT systems:

- a) The Processor uses logical access control with username and password or other unique authorization.
- b) The Processor uses antivirus programs that are updated regularly.
- c) The Processor requires employees to use individual passwords.
- d) The Processor's computers have automatic access protection during inactivity, ie. locked screen saver.
- e) The Processor has policies for password composition, including minimum requirements.
- f) The Processor logs and controls unauthorized or repeated failed login attempts.
- g) There are procedures for revoking permissions when an employee stops or switches department.
- h) There are procedures for granting authorizations to IT systems when hiring new employees.

Technical security: Access to personal data

The Processor shall implement the following technical security measures regarding access to personal data:

- a) The Processor has procedure(s) to restore data from backup.
- b) The Processor regularly reviews system controls.
- c) The Processor grants authorizations to individuals or groups of users to access, change and delete processed personal data.
- d) The Processor logs and controls unauthorized or repeated failed attempts to access data.
- e) The Processor logs and controls unauthorized or repeated failed attempts to erase data.
- f) The Processor has traceability of access, modification and erasure of data by individual users.
- g) The Processor regularly reviews and verifies user authorizations for specific systems.

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. Data is stored in the Microsoft Azure Data Center in the EU, where data is located in Amsterdam, the Netherlands and data backup takes place in Dublin, Ireland. (Read more here: Microsoft Azure Security and Rights Center: <https://azure.microsoft.com/en-us/support/trust-center/>).

Microsoft meets the most stringent security requirements and has the highest standards of certification: <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>

The access to data takes place via the website, which is hosted in Azure, and thus protected in accordance with all guidelines and standardized technologies from Microsoft. Passwords are hashed using with the strong hashing algorithm (SHA-256) with SALT and TLS 1.2 or higher (https) is used for all web calls.

Technical security: Encryption

The Processor shall implement the following technical security measures regarding encryption:

- a) The Processor's websites and web forms uses SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure).
- b) The Processor's computers have encrypted hard drives.
- c) The Processor encrypts personal data in systems and/or on devices.
- d) The network is encrypted.
- e) Passwords stored on the processor's computers, etc. are encrypted.

Technical security: Availability and robustness

The Processor shall implement the following technical security measures regarding availability and robustness:

- a) Accessibility and robustness of the processor's systems and servers are secured by a third party with whom the Processor has an agreement.
- b) Backups are made regularly (either in-house or at supplier).
- c) There are rules and guidelines for restoring data from backup.
- d) Only authorized employees have access to the Processor's own servers.
- e) Server rooms have smoke alarms and fire extinguishers.
- f) Server room has air conditioning system.
- g) There are rules and guidelines for data backup.
- h) Active alerting by unauthorized attempts to access server rooms and/or processing systems and data.
 - i) Uninterruptible power supply (UPS) is used.
 - j) Monitoring of temperature and humidity in server rooms.
- k) The processor has procedure descriptions for breaches of the personal data security that are reviewed at least annually.

3. Assistance to the Controller

3.1 The Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Controller in accordance with Clause [8.1](#) and [8.2](#) by implementing the following technical and organisational measures:

3.1.1 If the Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Processor, the Processor shall assist the Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

3.1.2 If the Controller needs the Processor's assistance in order to reply to a request

from a data subject, the Controller must send a written request for assistance to the Processor and the Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after receiving the request.

- 3.1.3 If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the request to The Controller.

4. Storage period/erasure procedures

- 4.1 After 3 years of inactivity from any survey participants personal data will automatically be anonymized to an irrevocable state (unless otherwise is agreed). The anonymized data will be kept for statistical purposes.

Upon request or on termination of the provisioning of technical data processing services (e.g. technical survey data) data will be anonymized no later than 30 days from termination notification. Due to system services such as Backup devices, data could remain in the systems for an additional 30 days. Summarized, the data to be anonymized could remain in the systems unmodified for up to 60 days, before it has been completed. Possible personal data processed, e.g. survey comments or answers to follow-up questions (all free-text fields) will be deleted within the 60 days, in accordance with paragraph 11.1.

5. Processing location

- 5.1 Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Controller's prior written authorisation:

At the Processor's own headquarter or at the headquarters of approved sub-processors as specified in Appendix B.

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

- 6.1 Personal data is only being processed by the Processor on the locations specified in clause [C.5](#).
- 6.2 If the Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Processor is not entitled to carry out such transfers within the scope of these Clauses.
- 6.3 Transfer of personal data can in all cases only be done in accordance with these Clauses, on the instructions of The Controller and to the extent permitted by the applicable data protection law.

- 6.4 Where, in accordance with these clauses, The Processor transfers personal data to sub-data processors in third countries outside the EU / EEA, the Processor must independently secure a legal basis for the transfer in accordance with Chapter 5 of GDPR.
7. **Procedures for the Controller's audits, including inspections, of the processing of personal data being performed by the Processor**
- 7.1 The Processor shall, upon the Controller's written request, document to the Controller that the Processor
- 7.1.1 is complying with his obligations under these Clauses and the Instruction, and
- 7.1.2 with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Controller.
- 7.2 According to Clause [C.7.1](#) The Processor's documentation shall be sent to the Controller within a reasonable time after receiving the request.
- 7.3 The processor must provide the controller with documentation of continuous compliance with the provisions. These self-audit reports must be prepared at least once a year and shall follow the principles and control objectives of the ISAE 3000 auditing standard, as laid down by Common Strategic Framework (CSF) - Danish Auditors and the Danish Data Protection Agency (and/or alternatively internationally recognized standards such as ISO/IEC 27701:2019). Self-audit reports may be conducted as part of the controller's information gathering and must be signed by the processor's management. The Processor is not obligated to initiate and undertake external audits of its compliance with the Clauses on its own initiative.
- 7.4 Regardless of Clause [C.7.3](#), The Processor shall furthermore provide for and contribute to audits and inspections every 12 months, performed by auditors appointed by the Controller, the public authorities in the competent jurisdiction, to the extent necessary to verify the Processor's compliance with these Clauses and the applicable data protection law. The auditor in question must be subject to confidentiality under law or agreement. The Controller must notify the audits in writing with 10 calendar days.
8. **Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors**
- 8.1 The Processor shall at least every 12th month, at their own expense, conduct an audit of the Processor's sub-processors and submit documentation for this audit to the Controller.
- 8.2 The Parties agree that the independent auditor's ISAE 3000 assurance report can be applied for this purpose.

Appendix D The Parties' terms of agreement on other subjects

1. Remuneration and costs

- 1.1 The Data Processor's compliance with these Clauses and time and material spent in connection herewith, shall only be separately payable if specified herein. The Parties agree that the Data Processor shall be entitled to invoice the Data Controller for used time and materials for performing works under the following clause(s) in the Clauses:
- The Data Processor's assistance in preparing impact assessments for the Data controllers and
 - The Data Processor's assistance with the Data Controller's compliance with the data subjects' rights.

The Data Processor is entitled to payment for the time and materials necessitated by and used to comply with any changes to the Instruction, when those changes are made by the Data Controller and are not a direct result of changes in Applicable Law.

If there are changes in the Applicable Law, including the interpretations hereof and issued guidelines from the relevant and applicable data protection agencies, any increased costs shall be born by each party respectively.