STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(g) These Clauses along with appendices shall be retained in writing, including electronically, by both parties.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

(a) In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law or other law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller

throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The data processor may with regards to "other law" only derogate from these Clauses if required to do so by other law to which the data processor is subject by virtue of being established in the third country, and if this other law is unlikely to have a substantial adverse effect on the rights and freedoms of the data subjects.

(c) Further, the data processor is - as part of the instructions form the data controller - entitled to anonymise personal data, and to process such anonymised data for the data processor's own purposes.

(d) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) The controller may only object to the use of a sub-processor if specific data protection issues related to the intended use of the sub-processor may constitute a violation of the data controller's obligations under applicable EU or Member State data protection provisions. The data processor must notify the data controller in writing upon termination of the use of a sub-processor.

(c) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(d) If the data processor engages or intends to engage a sub-processor for carrying out specific processing activities on behalf of the data controller, the data processor shall aim to impose on that sub-processor the same data protection obligations as set forth in these Clauses. If it, despite the data processor's efforts in good faith to do so, is not possible to impose these same obligations on the sub-processor, the data processor shall, as part of the submission required pursuant to Clause 7.7(a), notify the data controller hereof and submit the data protection-relevant parts of the data processor's agreement with the sub-processor to the data controller, cf. also Clause 7.7(g).

(e) The data controller acknowledges and accepts that these Clauses under the circumstances referred to in Clause 7.7(d), do not impose further data protection obligations on the data processor than those set out in the submitted agreement between the data processor and sub-processor. The data controller also acknowledges and accepts that the data controller may only object to the use of a sub-processor if specific data protection issues related to the intended use of the sub-processor may constitute a violation of the data controller's obligations under applicable EU or Member State data protection provisions, cf. Clause 7.7(b).

(f) Clause 7.7(d) and 7.7(e) also applies to the data controller's authorisation of the sub-processors listed in Annex IV at the time of conclusion of these Clauses.

(g) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(h) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(i) 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.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

(c) Subject to the data processor's compliance with Clauses 7.7 and 7.8, the data controller hereby authorises the data processor to establish a legal basis for transfers of personal data to third countries and organisations outside the EEA on behalf of and in the name of the data controller, including entering into standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR. The data processor is entitled to assign its rights under this Clause to sub-processors, whereas sub-processors may then on behalf of the data controller establish a legal basis for transfer of personal data to third countries and organisations outside the EEA, which includes entering into standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless

the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(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;

(2) the likely consequences of the personal data breach;

(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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay 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.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: LIST OF PARTIES

Controller(s):

1. Name: Customer name is set out in the Order.

Address: Customer adress is set out in the Order.

Contact person's name, position and contact details: Customer's contact point is set out in the Order.

Signature and accession date: *Signed together with the Order.*

Processor(s):

1. Name: Zero North A/S

Address: Amagerfælledvej 106, 4th floor, 2300 Copenhagen, Denmark

Contact person's name, position and contact details: Bo Kristensen, Chief Technology Officer, bo.kristensen@zeronorth.com

Signature and accession date: *Signed together with the Order.*

ANNEX II: DESCRIPTION OF THE PROCESSING

A) Noon Reports solution

Categories of data subjects whose personal data is processed

Customer's employees

Categories of personal data processed

Name, job function and emails of the employees of the Customer.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The processor will not process sensitive data.

Nature of the processing

The processing generally relates to the storage of the personal data as part of the noon reports.

 GDPR relevant data (vessel noon reports) is collected via our vessel web application hosted at https://vessel.noonreport.app/. The individual devices aboard a vessel will have their own logins as well as using the vessel IMO. The authentication setup is the same as for the rest of ZeroNorth's web applications (Auth0, SSO with Google)

 The responsible people aboard the vessel fill in the information in the web app, typically the chief engineer or the master. There are more than 300 data points in total to be reported. The relevant GDPR data points are:

- Captain's name
- Chief engineer's name
- Chief officer's name
- 2nd Engineer's name
- Nautical officer's name

 The data is accessible visible on the ZN platform - same security as mentioned before. Only accessible to the users who have a login for the platform for that specific customer.

Purpose(s) for which the personal data is processed on behalf of the controller

The noon reports are submitted to and stored by ZeroNorth as part of ZeroNorth Solution(s) as defined in the Agreement. The software requires vessel crew to report on relevant data points. Personal data included in the noon reports that falls under this agreement is the following:

- Captain name
- Chief engineer name

- Chief officer name
- 2nd Engineer name
- Nautical officer name

Duration of the processing

During the term of the Agreement with the Customer.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

Amazon Web Services EMEA SARL: AWS provides cloud services to the processor therefore all personal data processed on behalf of the controller is stored with AWS. When the agreement between the customer and ZeroNorth A/S is terminated or a user is deleted the personal data is also deleted from the cloud provided by AWS within one year after termination (in order for the processor to comply with its obligations under the agreement).

B) Bunker Platform solution

Categories of data subjects whose personal data is processed

The data controller's employees, including fuel brokers, buyers, suppliers, traders and contact persons.

Categories of personal data processed

Name, email address, company, job title, phone number, registered location and correspondence.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The processor will not process sensitive data.

Nature of the processing

The processor offers a a web-based Bunker Platform which handles all aspects of inquiry management from procument to payment. The processor's Bunker Platform drives industry best practice through workflows and audit trails. The Platform has built in email connectivity to make sure that the data controller and its employees are matched with suppliers or buyers at necessary ports. Further, the Platform manages confirmtions, amendments, claims, fuel tests, documentation and invoicing.

Purpose(s) for which the personal data is processed on behalf of the processor

The purpose of the processing is to registrer the employees of the data controller on the Platform and to provide the services available of the Platform.

The contact details are processed for the purpose of accessing the Platform and to contact other users of the Platform to enter into an agreement in relation to the provision of fuel. As the users will usually be employees of the data controller and enter into an agreement as a representative the users place of employment and title are processed to ensure, that other users know which company a person is representing and employed with.

The data subjects registered location is processed to ensure that the Platform matches the buyers and suppliers based on where the fuel is needed.

Furthermore, personal data may be processed for the purpose of anonymisation in order for the data processor to improve its platform by the use of anonymised data.

Duration of the processing

The personal data is processed on behalf of the processor until the main service agreement is terminated. If a user's employment ceased the controller or processor may either delete or have the sub-processor delete the specific user.

When the main agreement is terminated. The processor will return all personal data processed on behalf of the controller after which the processor will delete all personal data processed on behalf of the controller.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

ClearLynx: ClearLynx is the legal entity that has developed and is providing the provider of the Bunker Platform Solution.

Amazon Web Services, Inc.: AWS is a sub-processor to ClearLynx that provides cloud services to the processor therefore all personal data processed on behalf of the processor is stored with AWS.

When the agreement between the controller and ZeroNorth is terminated or a user is deleted the personal data is also deleted from the cloud provided by AWS within one year after termination (in order for the processor to comply with its obligations under the agreement).

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A) Noon Reports solution

Data is encrypted at all stages, in transit, at rest and in use.

Our software is designed and run according to our Information Security Management System (ISMS) which sets the requirements for confidentiality, availability and integrity.

Backups are encrypted and we have the ability to provision new environments and repopulate with data in case of incident.

Our platform is penetration tested by an Independent 3rd party at major release intervals and is assessed regularly for vulnerabilities.

Access to our software requires purchase of privisioned environment. Access to customer environments is agreed on setup and access is controlled via Auth0 and google SSO.

All data in transmission is encrypted.

Data at rest is also encrypted.

Our data resides in Amazon AWS data centres physically located in Ireland. The security of these data centres is in accordance with our ISMS.

All connections to and from systems are logged and alerts generated on thresholds or anomalies.

B) Bunker Platform solution

Data is encrypted at all stages, in transit, at rest and in use.

A contingency environment is available at all times in case of incident response or disaster recovery. This contingency environment includes all critical components of the application.

Our platform is penetration tested and a source code review is performed by an Independent 3rd party at least annually.

Infrastructure and application are assessed regularly for vulnerabilities.

All development follows a full software development life cycle process including code check-ins, static code analysis, compiled code vulnerability assessments and follows OWASP's guidelines.

Logins to the platform are secured with Multi Factor Authenication and upon the client's choice can be integrated with SSO.

Our data resides in Amazon AWS data centres physically located in the United States of America. AWS is ISO 27001 compliant.

All connections to and from systems are logged and alerts generated on thresholds or anomalies.

The processor will keep a list of persons to whom access has been granted pursuant to Clause 7.4(a) which shall be kept under periodic review by the processor. On the basis of this review, such access to personal data shall be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

A) Noon Reports solution

The controller has authorised the use of the following sub-processors:

1. Name: Amazon Web Services EMEA SARL

Address: 38 avenue John F. Kennedy, L-1855 Luxembourg

Contact person's name, position and contact details: …

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): AWS provides cloud hosting and stores the personal data processed on behalf of the controller.

B) Bunker Platform solution

The controller has authorised the use of the following sub-processors:

2. Name: ClearLynx

Address: 311 W43 St 13th Floor New York NY, 10036

Contact person's name, position and contact details: Kevin Arconti, IT and Security Manager, it@zeronorth.com.

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ClearLynx has developed and is providing the Bunker Platform solution to the controller through for processor.

The controller has authorised the use of the following entities acting as sub-processors for ClearLynx:

3. Name: Amazon Web Services, Inc.

Address: 410 Terry Avenue North, Seattle, WA 98109-5210

Contact person's name, position and contact details: N/A

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): AWS provides cloud hosting and stores the personal data processed on behalf of the controller.

Sub-processors engaged by Amazon Web Services

1) AWS infrastructure entities

The AWS entities listed below provide the infrastructure on which the AWS services run (including AWS Regions and Edge Locations). For more information about AWS's cloud

infrastructure, please see the AWS Global Infrastructure website. Where the AWS entity provides the infrastructure for an AWS Region, the AWS Region is listed below.

AWS entity	Processing location and associated AWS Region (if applicable)
A100 ROW GmbH	Germany AWS Region: Europe (Frankfurt)
A100 ROW Servicos De Dados Brasil Ltda.	Brazil AWS Region: South America (Sao Paulo)
A100 ROW, Inc.	USA
Amazon Asia-Pacific Resources Private Limited	Singapore AWS Region: Asia Pacific (Singapore)
Amazon Corporate Services Korea LLC	Korea AWS Region: Asia Pacific (Seoul)
Amazon Corporate Services Pty, Ltd	Australia AWS Region: Asia Pacific (Sydney)
Amazon Data Services Argentina S.R.L.	Argentina
Amazon Data Services Austria GmbH	Austria
Amazon Data Services Bahrain W.L.L.	Bahrain AWS Region: Middle East (Bahrain)
Amazon Data Services Belgium SRL	Belgium
Amazon Data Services Bulgaria LLC	Bulgaria
Amazon Data Services Canada, Inc.	Canada AWS Region: Canada (Central)
Amazon Data Services Colombia S.A.S.	Colombia

Amazon Data Services Czech Republic s.r.o.	Czech Republic
Amazon Data Services Denmark ApS	Denmark
Amazon Data Services Emirates LLC	United Arab Emirates
Amazon Data Services Estonia OÜ	Estonia
Amazon Data Services Finland Oy	Finland
Amazon Data Services France SAS	France AWS Region: Europe (Paris)
Amazon Data Services Greece Single-Member AE	Greece
Amazon Data Services Hong Kong Limited	Hong Kong AWS Region: Asia Pacific (Hong Kong)
Amazon Data Services Hungary Korlátolt Felelősségű Társaság	Hungary
Amazon Data Services, Inc.	USA AWS Region: US East (Northern Virginia) / US East (Ohio) / US West (Northern California) / US West (Oregon)
Amazon Data Services India Private Limited	India AWS Region: Asia Pacific (Mumbai)
Amazon Data Services Ireland Limited	Ireland AWS Region: Europe (Ireland)
Amazon Data Services Israel Ltd	Israel
Amazon Data Services Italy S.R.L	Italy AWS Region: Europe (Milan)

Amazon Data Services Japan G.K.	Japan AWS Region: Asia Pacific (Osaka) / Asia Pacific (Tokyo)
Amazon Data Services Kenya Limited	Kenya
Amazon Data Services Malaysia Sdn. Bhd.	Malaysia
Amazon Data Services MX, S. de R.L. de C.V.	Mexico
Amazon Data Services Netherlands N.V.	Netherlands
Amazon Data Services New Zealand Limited	New Zealand
Amazon Data Services Norway AS	Norway
Amazon Data Services Panama, S. de R.L.	Panama
Amazon Data Services Portugal, Lda	Portugal
Amazon Data Services Romania S.R.L.	Romania
Amazon Data Services South Africa (Pty) Ltd	South Africa AWS Region: South Africa (Cape Town)
Amazon Data Services Spain, S.L.U.	Spain
Amazon Data Services Sweden AB	Sweden AWS Region: Europe (Stockholm)
Amazon Data Services Switzerland GmbH	Switzerland
Amazon Data Services Taiwan Limited	Taiwan
Amazon Data Services (Thailand) Limited	Thailand

Amazon Data Services UK Limited	UK AWS Region: Europe (London)
Amazon Data Services Zagreb d.o.o.	Croatia
Amazon Technological Services SAS	France AWS Region: Europe (Paris)
Amazon Web Services Philippines, Inc.	Philippines
Amazon Web Services Poland sp. z o.o.	Poland
PT Amazon Data Services Indonesia	Indonesia
Servicios Amazon Data Services Chile SpA.	Chile
Servicios Amazon Data Services Peru SRL	Peru

2) AWS service providers

The AWS entities listed below provide processing activities for specific AWS services. The processing activities provided by the AWS entities include selling and providing certain business application, application integration, and media services (application and media services), human transcription of voice recordings (transcription services), development and improvement of AWS services (service improvement), and/or customer-initiated support.

a) AWS entities selling and providing application and media services
The AWS entities that sell and provide application and media services are listed below along with the associated services. The processing location is the customer's selected AWS Region(s), and the location of the customer's end users.

AWS entity	AWS service(s)	Processing activity
AMCS LLC (USA)	Alexa for Business Amazon PSTN Chime Amazon PSTN Connect	Seller and provider of the AWS service listed to the left for all customers (except for customers based in Singapore)
	Amazon Chime AWS Elemental MediaConnect Amazon Pinpoint	Seller and provider of the AWS services listed to the left for customers based in Japan

	Amazon Simple Email Service Amazon Simple Notification Service Amazon WorkDocs	
AMCS SG Private Limited (Singapore)	Amazon Chime Amazon Connect Amazon Pinpoint Amazon Simple Email Service Amazon Simple Notification Service	Seller and provider of the AWS services listed to the left for customers based in Singapore

b) AWS entities providing service improvement

Unless customer opts out of AWS using Customer Data for service improvement, where permitted in accordance with the AWS Service Terms, the AWS entities listed below provide service improvement for the applicable AWS services.

AWS entity	AWS service(s)	Processing location	Processing activity
Amazon Development Centre (India) Private Limited	Amazon Lex Amazon Transcribe	India	Service improvement
Amazon Web Services, Inc.	Alexa for Business Amazon AppStream 2.0 User Pool Amazon CodeGuru Profiler Amazon Comprehend Amazon Connect Customer Profiles Identity Resolution Amazon Fraud Detector Amazon GuardDuty* Amazon Lex Amazon Polly Amazon Rekognition Amazon Textract Amazon Transcribe Amazon Translate	USA	Service improvement

	Contact Lens for Amazon Connect		

*To the extent that the Amazon GuardDuty Malware Protection feature is enabled.

c) AWS entities providing customer-initiated support

The AWS entities listed below provide customer-initiated support. These entities do not process Customer Data unless the customer agrees to share Customer Data in the course of requesting support.

AWS entity	Processing location (if applicable)
Amazon.com Services LLC	USA
Amazon Data Services SA (Pty) Ltd	South Africa
Amazon Development Centre (India) Private Limited	India
Amazon Development Centre Ireland Limited	Ireland
Amazon Development Centre (South Africa) (Proprietary) Limited	South Africa
Amazon Internet Services Private Limited	India
Amazon Support Services Costa Rica, SRL	Costa Rica
Amazon Web Services Australia Pty Ltd	Australia
Amazon Web Services Canada, Inc.	Canada
Amazon Web Services EMEA SARL	France and Ireland
Amazon Web Services Hong Kong Limited	Hong Kong
Amazon Web Services Japan KK	Japan

Amazon Web Services Korea LLC	Korea
Amazon Web Services Taiwan Ltd	Taiwan
Amazon Web Services, Inc.	USA
AWS India ProServe LLP	India
Elemental Technologies LLC	USA
Souq.com for E-Commerce LLC	Egypt

3) Third-party service providers

AWS has contracted with the following unaffiliated service providers for Application-to-Person (A2P) messaging services and geolocation services (such as maps or points of interest) for the AWS services described below. The processing location is the customer's selected AWS Region(s), the service provider's location listed below and/or the location of the customer's end users.

Service provider	AWS service(s)	Service provider's location	Processing activity
250ok Inc.	Amazon Pinpoint	USA	A2P messaging
Bandwidth Inc.	Amazon Chime	USA	A2P messaging
Email Data Source, Inc.	Amazon Pinpoint	USA	A2P messaging
Environmental Systems Research Institute, Inc.	Amazon Location Service	USA	Geolocation (maps and points of interest)
HERE North America, LLC	Amazon Location Service	USA	Geolocation (maps and places)

Infobip Ltd.	Amazon Pinpoint Amazon Simple Notification Service	United Kingdom	A2P messaging
Nexmo Inc.	Amazon Pinpoint Amazon Simple Notification Service	USA	A2P messaging Phone number validation
Sinch Americas Inc.	Amazon Pinpoint Amazon Simple Notification Service	USA	A2P messaging
TeleSign Corporation	Amazon Pinpoint Amazon Simple Notification Service	USA	A2P messaging Phone number validation
Twilio, Inc.	Amazon Pinpoint Amazon Simple Notification Service	USA	A2P messaging

Last Updated: 9 August 2022

ANNEX V (ONLY APPLICABLE TO NON-EU/EEA CUSTOMERS): EU COMMISSION STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES PURSUANT TO REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (PROCESSOR-TO-CONTROLLER)

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(a) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex V.I.A. (hereinafter each "data exporter"), and

(b) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex V.I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex V.I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(a) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(b) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(c) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(d) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(e) Clause 13;

(f) Clause 15.1(c), (d) and (e);

(g) Clause 16(e);

(h) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex V.I.B.

Clause 7 - Optional

Docking clause

(d) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex V.I.A.

(e) Once it has completed the Appendix and signed Annex V.I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex V.I.A.

(f) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(g) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(h) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(i) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(j) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

Not applicable.

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

Not applicable.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(f) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not

exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(g) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(a) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(b) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(c) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(h) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(i) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(j) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(k) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(a) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(b) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These

requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(a) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(b) the data importer is in substantial or persistent breach of these Clauses; or

(c) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

APPENDIX

ANNEX V.I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Zero North A/S

Address: Amagerfælledvej 106, 4th floor, 2300 Copenhagen, Denmark

Contact person's name, position and contact details: Bo Kristensen, Chief Technology Officer, bo.kristensen@zeronorth.com

Activities relevant to the data transferred under these Clauses: See Annex II.

Signature and date: *Signed together with the Order*

Role (controller/processor): Processor

Data importer(s):

1. Name: Customer name is set out in the Order.

Address: Customer adress is set out in the Order.

Contact person's name, position and contact details: Customer's contact point is set out in the Order.

Activities relevant to the data transferred under these Clauses: See Annex II.

Signature and date: *Signed together with the Order.*

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Annex II.

Categories of personal data transferred

See Annex II.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Annex II.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continous basis.

Nature of the processing

See Annex II.

Purpose(s) of the data transfer and further processing

See Annex II.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Annex II.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex IV