GENERAL TERMS AND CONDITIONS

Unless otherwise defined or the context otherwise requires, capitalised terms used in the Agreement shall have the following meaning:

Affiliate means any Person or legal entity which, whether through ownership or otherwise, Controls, is Controlled by, is under common Control with, or which is managed by a Party (or, if the context so requires, a Person in question).

Agreement means an Order, these T&Cs, the applicable Service Description(s), the data processing agreement, the standard contractual clauses, and any applicable Product Terms.

Charges means the charges for the Services and Solutions set forth in the Order.

Clause means any clauses in the Agreement.

Commencement Date means the date when Supplier makes the Solution(s) and the Services available to Customer as set out in the Order.

Confidential Information has the meaning ascribed to it in Clause 23.

Control with respect to any Person (the "Relevant Person"), the power or ability (directly or indirectly) to direct the affairs of that Relevant Person (whether by means of ownership, contract or otherwise), and **Controlled** and **Controlling** will be construed accordingly, provided that in any event, any person that (i) owns directly or indirectly securities having more than 50% of the voting power for the election or removal of directors (or other equivalent governing body) of that Relevant Person or that (ii) holds beneficially more than 50% of the ownership interests of that Relevant Person shall, in either such case, be deemed to Control that Relevant Person.

Customer has the meaning ascribed in the Order.

Customer Data means all data which Customer has provided to Supplier, including provided for the use by, in, or in relation to the Solutions or the Services, in each case regardless of whether provided or generated before or after the conclusion of the Agreement. For the avoidance of doubt, to the same extent, such Customer Data shall also include any Customer Intellectual Property Rights incorporated or embedded therein.

Data Protection Laws means (a) relevant United States privacy laws, including the California Consumer Privacy Act; and (b) the EU General Data Protection Regulation (2016/679).

Effective Date has the meaning ascribed in the Clause 18.1.

Good Industry Practice means the exercise of the degree of skill, diligence, prudence, efficiency, foresight and timeliness which would be expected from a proper qualified and competent person or organization within the relevant industry or business sector.

Intellectual Property Rights means (i) industrial and intellectual property rights throughout the world, including all copyrights, mask works, moral rights, rights affording protection similar to copyright, rights in databases, letters patents, patent rights, utility models, and rights in inventions, semi-conductor topography rights, trade marks, trade dress, rights in internet domain names and website addresses and other rights in trade names, registered designs, design rights, know-how, trade secrets and other rights in confidential information, including under marketing legislation, (ii) applications for registration, and the right to apply for registration, for any of the rights listed in item (i) whether or not registered or registerable, including all granted registrations and all applications for registration, in any country or jurisdiction, and (iii) all other rights having equivalent or similar effect in any relevant country or jurisdiction in the world.

Order means the written order governing Customer's subscription to the Solution(s) and Services.

Parties means Customer and Supplier collectively.

Party means either Customer or Supplier.

Person means any individual, company, partnership, joint venture, firm, association, trust, governmental or regulatory authority or other body or entity (whether or not having separate legal personality).

Personal Data any information considered "personal data," "personal information," "personally identifiable information," or any similar terms under applicable Data Protection Laws..

Product Terms means any specific terms related to a specific Solution (and related Services) provided by Supplier to Customer (as updated from time to time by Supplier).

Services means Supplier's services set out in the Service Description(s) provided by Supplier under the Agreement, including Customer's right to access and use the Solutions.

Service Description means Supplier's service description linked to in the Order.

Solution(s) means Supplier's solutions Customer has subscribed to under the Order, including any add-on modules to such Solutions which Customer has subscribed to.

Supplier means Clearlynx LLC.

Term means, collectively, the initial term of the Agreement and any subsequent renewal terms.

T&C means these general terms and conditions.

1 SCOPE OF THE AGREEMENT AND ORDERING

1.1 Supplier shall provide Customer with access to the Solutions and deliver the Services to Customer as set out in the Order and in accordance with the terms and conditions of the Agreement. The Order can be entered into directly between Supplier and Customer or between one of Supplier's Affiliates (on behalf of Supplier) and Customer. No matter if the contractual party to the Order is Supplier or one of Supplier's Affiliates, the Solution(s) and Services will be delivered directly from Supplier to Customer and Supplier's Affiliate will only enter into the Order on behalf of Supplier and will therefore not act as a reseller of the Solution(s) and Services to Customer (i.e. the Agreement shall always be considered a direct agreement between Supplier and Customer governing Customer's use of the Solution(s) and Services). If the Order governs Customer's subscription to both Supplier's Solution(s) and Services and Supplier's Affiliate(s)' solution(s) and services, Supplier will be the Supplier of the Solution(s) and Services and the applicable Supplier Affiliate will be supplier of its own solutions and services to Customer.

1.2 The Solutions and Services shall be supplied in accordance with Good Industry Practice.

1.3 To the extent Customer wishes to purchase additional services or subscribe to other solutions delivered by Supplier, the Parties shall enter into a new agreement governing such additional purchase.

1.4 Customer's subscription to the Solution(s) and Services shall be governed by the terms and conditions of these T&Cs, unless deviated from or supplemented in the Order or in the Product Terms.

2 CUSTOMER'S ACCESS AND RIGHTS TO USE THE SOLUTIONS

2.1 Unless stated otherwise in the Order, and in accordance with the terms and conditions of the Agreement, Supplier, in consideration for the Charges, hereby grants to Customer and its Affiliates a non-exclusive, non-transferrable, non-sublicensable, revocable, worldwide right and license to access the Solutions and use the Services during the Term solely for Customer's and its Affiliate's internal business purposes and in accordance with the Agreement and subject to any restrictions and limitations otherwise set out in the Order or Product Terms.

2.2 Customer may freely increase its amount of use of the Solutions and Services in exchange for increased Charges, as set out in the Order.

2.3 Customer, on behalf of itself and its Affiliates, acknowledges and agrees that it and they will not use the Solutions or Services to form part of a service bureau or outsourcing an offering by Customer or its Affiliates to third parties.

2.4 In order to make use of the Solutions and Services Customer acknowledges and agrees that it must provide the data pertaining to the relevant Solution or Service and comply with the technical requirements for the relevant Solution or Service. The necessary data and technical requirements as of

the Effective Date are set out in the applicable Product Terms.

2.5 Customer and its Affiliates shall not, and Customer represents and warrants that it and its Affiliates will not:

(i) sell, resell, distribute, rent or lease the Solutions or Services or use the Solutions or Services for the benefit of any Person other than Customer and its Affiliates;

(ii) use the Solutions to store or transmit infringing, misappropriating, libellous or otherwise unlawful or tortious material;

(iii) use the Solutions or Services in any way that violates any applicable federal, state, local or international law or regulation (including, without limitation, any laws regarding export of data or software to and from the US or other countries);

(iv) use the Solutions to store or transmit any material in violation of any third-party rights;

(v) interfere with or disrupt the integrity or performance of any Solution, Service or third-party data contained therein;

(vi) take any actions that affect Supplier's right, title or interest in the Solutions or Services;

(vii) give access to the Solutions or Services to any third party without Supplier's prior written consent;

(viii) remove, alter or obscure, any proprietary notices and licenses on the Solutions or Services;

(ix) separate or uncouple any portions of the Solutions or Services, in whole or in part, from any other portions thereof; and

(x) modify, create derivative works of, reverse assemble, reverse engineer, translate, disassemble, decompile or otherwise attempt to create or discover any source code, underlying algorithms, ideas, file formats, programming interfaces of or other works from, or analyze to determine their composition or physical structure or perform destructive testing on, the Solutions or Services by any means whatsoever, without the prior written approval of Supplier, save as permitted by applicable law.

2.6 Supplier may suspend Customer's access to the Solution and Services, with or without notice, at any time if, Supplier in its reasonable opinion believes that Customer or its users have violated any provision in the Agreement, including if Customer has not paid the Charges.

3 DIVESTURE

3.1 In the event that (i) an Affiliate of Customer is divested to a third party, or (ii) Customer or an Affiliate divests a business unit or activity in the form of a transfer of assets, Customer shall be entitled to allow the divested Affiliate or business unit (or the buyer) at no additional charge to continue accessing the Solutions and using the Services for a period of twelve (12) months from the date of closing of the transaction concerning transfer of the Affiliate or business unit. Customer shall be liable for such continued access/use by the divested Affiliate or business unit and the access/use shall otherwise remain subject to the terms and conditions agreed herein.

3.2 In the event that (i) an Affiliate of Customer is divested to a third-party, or (ii) Customer or an Affiliate divests a business unit or activity in the form of a transfer of assets, Customer shall be entitled to partially assign its rights and obligations under the Agreement to the divested Affiliate or the buyer of the business unit/activities (as the case may be) at no additional charge, provided that the assignee adheres to the Agreement and has the sufficient financial standing to honour the obligations undertaken under the Agreement. As part of the said assignment, the Parties shall agree on the relevant modifications in respect of split of Charges and other relevant changes occurring as a consequence of such transfer.

4 DEVELOPMENT, MAINTENANCE AND TECHNICAL SUPPORT

4.1 The Services are described in the Service Description and Product Terms.

4.2 Regardless of any further development, Supplier will in all material respects maintain the existing core functionality of the Solutions as of the Effective Date.

4.3 Customer may propose changes to a Solution and/or Services, including development of new functionality, however, any changes to or development of a Solution or Services shall be at Supplier's sole discretion.

4.4 The Solutions will automatically be updated by Supplier at no additional charges when new versions, updates, service packs, releases or hot-fixes are available, thus Customer will always be upgraded to the latest version of the applicable Solution without prior notice and without consent (One Version Policy). Such new versions, updates, etc. will be subject to the terms and conditions of the Agreement and considered an integrated part of the applicable Solution. However, see also Clause 4.5.

4.5 Supplier may develop new modules or products, which, at Supplier's sole discretion, may be separately marketed and priced, and which are not part of the Solutions or Services already purchased by Customer under the Order.

4.6 Supplier may amend the Product Terms (e.g. in case of changes to a Solution or Service). In case of material changes, Supplier will provide prior written notice to Customer and Customer shall be entitled to terminate the applicable Solution or Service for convenience with immediate effect within 30 days following Customer's receipt of such notice.

4.7 Supplier shall as part of the Services maintain and, at Customer's request, provide to Customer, a back-up of any and all Customer Data and other data in the Solutions required for Customer's continuation of business, including in the event of disaster recovery.

5 USE OF SUB-SUPPLIERS

5.1 Supplier may subcontract all or part of the Services without Customer's prior written consent. Furthermore, Supplier may change a sub-supplier without obtaining Customer's approval.

5.2 The subcontracting will not relieve Supplier of its obligations under the Agreement. Supplier shall be responsible for all acts and omissions of its sub-suppliers as if they were Supplier's own.

5.3 Notwithstanding Clause 5.2, to the extent Supplier uses material sub-suppliers, (e.g. to provide cloud infrastructure services), the liability caused by use of such material sub-suppliers' shall be subject to the limitations set out in the terms and conditions of the material sub-suppliers. Supplier shall pass through to Customer any compensation received under warranties and indemnities offered by the material sub-supplier. If more customers have been affected, such compensation shall be distributed between the affected customers. Material sub-suppliers are set out in the Product Terms or the Service Description (as updated from time to time).

6 CONSULTANCY SERVICES

6.1 Customer may request changes to a Solution and/or Services, including development of new functionality, however, any changes to or development of a Solution or Services shall be at Supplier's sole discretion. Such development shall be described and agreed in a separate statement of work entered into between the Parties governing such consultancy services. When such changes to a Solution or Service is released in accordance with the applicable statement of work, the changes will form an integrate part of the applicable Solution or Service and will be governed by the terms and conditions of these T&C, unless explicitly deviated from or supplemented in such statement of work.

6.2 As between the Parties, Supplier reserves all right, title and interest in and to all Intellectual Property Rights and other rights, title and interest in such developments, improvements, design contributions or derivative works thereto and such may, at Supplier's sole discretion, be made generally available in the Solutions (to other customers), at no additional charges or separately marketed and priced.

6.3 Any additional consultancy services to be delivered by Supplier will be performed on a time and material basis and subject to Supplier's applicable hourly rates. Supplier's standard consultancy terms and conditions shall apply to such services.

7 INTELLECTUAL PROPERTY RIGHTS

7.1 As between the Parties, Supplier reserves all right, title and interest in and to all Intellectual Property Rights and other rights, title and interest in the Solutions and Services, any improvements, design contributions or derivative works thereto and all data generated by the use of the Solutions and Services.

7.2 In case third-party software or data is incorporated into the Solutions or Services by Supplier, the third-party's terms relating to such third-party software or data will

apply to such third-party software or data. It is Customer's responsibility to ensure it complies with such third-party terms. If Supplier's agreement with any third-party software or data provider is terminated (i.e. also third-party providers not listed in the Agreement), Supplier shall endeavor to replace the third-party provider with a provider of similar third-party data or software. If Supplier cannot replace the third-party provider and such third-party data or software is material for Customer's use of a Solution or Service, Customer shall be entitled to terminate such Solution or Service for convenience with immediate effect.

7.3 Customer hereby grants Supplier a non-exclusive, irrevocable, transferrable, sublicenseable, royalty-free, fully-paid, worldwide right and license, as of the Effective Date, to all Customer Data, for Supplier to use and otherwise exploit in any manner it sees fit; provided, however, Supplier may only disclose such Customer Data to third parties, if such Customer Data is anonymized beforehand. Save as set out in the Agreement Customer waives absolutely and irrevocably against Supplier any and all rights, objections or claims, including any Intellectual Property Rights, relating to Supplier's use of Customer Data in accordance with this Clause 7.

7.4 Notwithstanding Clause 7.3, Customer hereby grants Supplier an exclusive, irrevocable, transferrable, sublicenseable, royalty-free, fully-paid, worldwide right and license, as of the Effective Date, to all Customer Data, for Supplier to use and otherwise exploit in any manner it sees fit within Supplier's field of use during the Term and for a period of three (3) years following the Term provided, however, Supplier may only disclose such Customer Data to third parties, if such Customer Data is anonymized beforehand. For the avoidance of doubt, this provision shall not limit Customer's right to subscribe to third-party solutions similar to the Solutions and Services.

7.5 Notwithstanding Clause 7.3, in case Customer has provided Customer Data not owned by Customer, Customer shall notify Supplier of such ownership issue and procure the rights necessary to grant the license granted in Clause 7.3.

8 COMPLIANCE WITH LAWS

8.1 Supplier shall comply with mandatory regulatory requirements under applicable law generally applicable to Supplier as an IT provider.

8.2 Customer shall be responsible for ensuring compliance with any local or industry specific regulatory requirements and for informing Supplier of any such requirements and how to implement them in the Solutions and Services, if required. However, Supplier is not obliged to implement such local or industry specific regulatory requirements in the Solutions or Services.

9 SANCTIONS

9.1 Each Party will comply with any (trade) sanction laws applicable and, in particular any law enforced by the US, the United Kingdom, Denmark and/or the EU.

9.2 A Party shall be entitled to terminate the Agreement with immediate effect in the event that the Agreement will place such Party in non-compliance with any (trade) sanction laws applicable and, in particular any laws enforced by the US, the United Kingdom, Denmark and/or the EU.

10 DATA PROTECTION AND SECURITY

10.1 If Supplier shall process Personal Data on behalf of Customer, the Parties shall enter into a data processing agreement. To the extent applicable, Supplier will at all times comply with all applicable Data Protection Laws, in relation to all Personal Data to which it has access in the course of performing its obligations under the Agreement.

10.2 The level and extent of IT security measures shall comply with Good Industry Practice and applicable regulatory requirements.

11 AUDIT

11.1 Supplier may, at its expense and no more than once every 12 months, appoint its own personnel or an independent third party (or both) to verify that Customer's use, installation, or deployment of the Solutions and Services comply with the terms of the Agreement. Customer shall provide all reasonable information and assistance requested by Supplier.

11.2 In the event that Customer's use of a Solution or a Service is in violation of the Agreement, e.g. misuse of the license keys, Customer shall immediately settle underpayment on the basis of the current Charges and Customer shall pay all reasonable expenses incurred by Supplier related to such audit. In addition, Supplier is entitled to claim additional losses and damages recoverable under law.

12 CHARGES

12.1 The Charges for Customer's subscription to Solutions or Services are specified in the Order.

12.2 Supplier reserves the right to change or modify the Charges upon 45 days prior written notice to Customer. Customer's continued use of the Solutions and Services after the expiration of the 45 days following Customer's receipt of such notice shall constitute Customer's acceptance of and agreement to be bound by Suppliers modified Charges for the Solutions and Services.

13 PAYMENT

13.1 Charges for Solutions and Services will be invoiced as set out in the Order. In the absence of such regulation, invoicing will take place in arrears based on Charges incurred in the preceding quarter.

13.2 Payment must take place no later than current month + thirty (30) days after Customer has received the invoice.

13.3 In case of delayed payment, Supplier is entitled to interest at the rate of 1.5 % per commenced month on the outstanding amount from the due date until the date of payment.

13.4 All Charges are exclusive of VAT and shall be paid in U.S. Dollars, except as otherwise stated in the Order.

13.5 Customer is responsible for any local usage, valued added, or other tax levied by a taxing authority with jurisdiction over Customer. Fees paid to Supplier are exclusive of any such taxes and Supplier shall have no obligation to calculate or pay any such fees for which Customer may be liable, provided however, that Supplier may charge Customer sales tax for any goods or services and in any jurisdiction in which Supplier is obligated to do so.

14 WARRANTIES

14.1 During the Term, Supplier warrants that:

(i) it has and will maintain all necessary licenses, consents, and permissions necessary for the performance of its obligations under the Agreement; and

(ii) Supplier complies with law applicable to Supplier.

14.2 The warranties above do not apply to defects or errors which are results of deliverables from Customer or third parties for which Customer is responsible.

14.3 Supplier shall at its expense remedy any breach of the warranties in Clause 14.1 in accordance with the maintenance requirements set out in Clause 4.

15 LIABILITY

15.1 Except for breaches of Clauses 2.3, 2.5, 7.3-7.5, 9, 16, and 23, the aggregate liability of a Party under the Agreement shall in no event exceed an amount equal to 100 % of the total Charges paid by Customer in the twelve (12) months period preceding the date of the first claim made for the Solution (including Services) in question. If the Agreement has not been in force twelve (12) months at the time of occurrence of the breach for which the first claim is made, the "total Charges" shall be deemed to include all Charges paid for the actual period lapsed for such Solution and multiplied with a factor to correspond to a twelve (12) month period. The above limitation of liability shall not apply to Charges payable by Customer.

15.2 The limitation of liability will apply to any and all liability irrespective of the basis of liability, i.e. damages, proportionate reduction, penalties, and indemnity.

15.3 Except for breaches of Clauses 2.3, 2.5, 7.3-7.5, 9, 16, and 23, the Parties shall not be liable for indirect losses or consequential damages of any kind, including, but not limited to, loss of profits, loss of business or revenue, loss of goodwill or data, or loss related to processing of Personal Data unless otherwise provided in the Agreement.

15.4 The Parties agree that any damage and loss incurred by a Party due to liability arising from (i) fraudulent misrepresentation, willful misconduct or gross negligence, or (ii) personal death or bodily injury shall not be limited in any way by Clauses 15.1 and 15.3 or by any other Clause of the Agreement, except for Clause 17.1.

16 INDEMNIFICATION

16.1 A Party shall indemnify the other Party or its Affiliates in respect of fines, penalties, damages awarded or any settlement amount agreed and reasonable legal and other professional fees and any other documented cost incurred by or awarded against the relevant Party in connection with (i) a third-party claim relating to infringement of third-party intellectual property or other rights, including patents and copyrights with respect to hardware, software and other materiel provided by or through the other Party under the Agreement and (ii) breach of the confidentiality obligations in Clause 23.

16.2 The obligations under this Clause 16 in relation to third-party claims are conditional upon (a) the Party against whom a third-party claim is brought timely notifying the other Party in writing of any such claim, provided however that a Party's failure to provide or delay in providing such notice shall not relieve a Party of its obligations under this Clause 16 except to the extent such failure or delay prejudices the defense; (b) the Party who is obligated hereunder to defend a claim having the right to fully control the defense of such claim; and (c) the Party against whom a third-party claim is brought reasonably cooperating in the defense of such claim. Neither Party shall undertake any action in response to any infringement or alleged infringement that is prejudicial to the other Party's rights.

17 DISCLAIMER

17.1 EXCEPT FOR THE WARRANTIES SET FORTH IN SECTION CLAUSE 14.1, SUPPLIER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, AS TO ANY MATTER WHATSOEVER, INCLUDING WITH RESPECT TO THE SOLUTIONS AND THE SERVICES, AND INCLUDING THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COMPLETENESS, SECURITY, QUALITY, ACCURACY, PERFORMANCE, AND FITNESS OF USE.

17.2 WITHOUT LIMITING THE FOREGOING, SUPPLIER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, THAT THE SOLUTION, ITS CONTENT OR ANY SERVICES OR ITEMS OBTAINED THROUGH IT WILL BE ACCURATE, RELIABLE, ERROR-FREE OR UNINTERRUPTED, THAT DEFECTS WILL BE CORRECTED, THAT THE SOLUTION IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR THAT THE SOLUTION OR ANY SERVICES OR ITEMS OBTAINED THROUGH IT WILL OTHERWISE MEET THE CUSTOMER'S NEEDS OR EXPECTATIONS.

17.3 The Solutions and Services rely on and provide data from a variety of different data sources. Customer acknowledges and accepts that such data may not reflect the latest real-time situations.

17.4 Notwithstanding anything to the contrary in the Agreement, any third-party data incorporated by Supplier in the Solutions or Services is provided "as is". Supplier does not warrant the completeness or accuracy of the data, material, third party advertisements or information or that it will satisfy Customer's requirements. Supplier disclaim all other express or implied warranties, conditions, and other terms in relation to such third-party data, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to quality, merchantability, fitness for a particular purpose and non-infringement.

17.5 Customer acknowledges and accepts that while due care and skill has been used, Supplier provides no warranties or representation that any price indications, quotes or any other calculations or assessments provided by or through the Solutions and Services will reflect actual prices, circumstances, etc. and be obtainable by the Customer.

17.6 Customer hereby releases Supplier and its Affiliates from any and all liability related to personal or property damages of any crew or any vessel, including damage to cargo, personal death, and bodily injury. Customer acknowledges and accepts that any decision concerning its vessels and crew is undertaken solely by Customer and that Solutions and Services are provided for reference only and shall in no way substitute sound judgment.

18 TERM AND TERMINATION FOR CONVENIENCE

18.1 The Agreement becomes effective when the Order is duly signed (the "**Effective Date**"). The Commencement Date and initial term are set out in the Order.

18.2 Unless terminated by either Party in accordance with Clause 18.3 the Agreement will automatically renew for periods of twelve (12) months following (i) the initial term or (ii) any subsequent renewal period.

18.3 A Party is entitled to terminate the Agreement in whole or in part for convenience with a written notice of at least ninety (90) days to the end of the initial term or a subsequent renewal period.

19 TERMINATION FOR CAUSE

19.1 A Party may terminate the Agreement, in whole or in part, immediately or by giving up to thirty (30) days' written notice of termination to the other Party if one or more of the following circumstances occurs:

(i) The other Party commits a breach of the Agreement, which is not insignificant, and, provided the breach is capable of remedy, the Party in question has failed to remedy that breach within thirty (30) days following receipt of a written notice from the other Party to do so; and/or

(ii) The other Party commits a material breach of the Agreement, which is not capable of remedy.

19.2 In the event of termination or expiry of the Agreement, howsoever occurring, Supplier shall upon Customer's request provide all necessary termination assistance until a copy of all Customer Data has been transferred to Customer or a replacement service provider designated by Customer in the same format as Customer Data was delivered to Supplier. Any such termination assistance shall be chargeable by Supplier on a time and material basis. Subject to Customer's payment of the Charges, Supplier shall be obliged to continue its provision of the Services temporarily until such successful transfer has been achieved.

19.3 Termination of the Agreement shall not affect either Party's rights and duties under Clauses 2.3, 2.5, 6.2, 7, 15 – 17, 19.3, 20 – 28, and all defined terms shall survive.

20 CONTRACT DOCUMENTS AND INTERPRETATION

20.1 A reference to "includes" or "including" shall mean "includes without limitation" or "including without limitation".

20.2 The Agreement supersedes all prior agreements and understandings between the Parties with respect to the Solutions and the Services.

20.3 If any Product Terms apply to a Solution or a Service provided by Supplier to Customer, such specific terms shall take precedence over these T&Cs.

21 SEVERABILITY AND WAIVER

21.1 If any term in the Agreement is found by competent judicial authority to be unenforceable in any respect, the validity of the remainder of the Agreement will be unaffected, provided that such unenforceability does not materially affect the Parties' rights under the Agreement.

21.2 An effective waiver under the Agreement must be in writing signed by the Party waiving its right. Hence, the failure of a Party to exercise any right or remedy to which it is entitled will not constitute a waiver of such right or otherwise cause a diminution of the obligations created by the Agreement, unless explicitly agreed to in writing. Furthermore, a waiver by either Party of any instance of the other Party's noncompliance with any obligation or responsibility under the Agreement will not be deemed a waiver of subsequent instances.

22 FORCE MAJEURE

22.1 Either Party is entitled to suspend the performance of its obligations without incurring liability for damages under the Agreement if and to the extent that such performance is impossible due to extraordinary circumstances beyond the reasonable control of such Party and such circumstances could not have been foreseen and avoided, including by virtue of business continuity plans, contingency plans, disaster recovery plans or other similar preventive measures in accordance with Good Industry Practice.

22.2 The Party claiming to be affected by any circumstance referred to in Clause 22.1 shall, without undue delay, notify the other Party of the intervention and of the cessation of such circumstance.

22.3 Notwithstanding any other provisions of the Agreement, either Party is entitled to terminate the Agreement with immediate effect by written notice to the other Party if it is clear from the circumstances that the performance of the Agreement will be and

is suspended under Clause 22.1 for more than 30 days.

23 CONFIDENTIALITY

23.1 The Parties shall not, apart from what is required by applicable law or by any court or other authority of competent jurisdiction, make use of, except for the purposes contemplated by the Agreement, disclose to any third party or publish any Confidential Information received by one Party from or in respect of the other Party under or in connection with the Agreement. The receiving Party will use the same care and discretion to avoid disclosure, publication, or dissemination of the disclosing Party's Confidential Information as the receiving party uses with its own Confidential Information, but in any event, no less than a reasonable standard of care.

23.2 For the purpose of the Agreement, "Confidential Information" means a Party's trade secrets as well as other commercial and operational information and knowhow and any other information not generally known or reasonably ascertainable.

23.3 The Parties shall ensure that their Affiliates, and its and their employees, also observe this Clause 23.

23.4 This Clause 23 shall not apply to information that is: (a) in the public domain through no fault of the receiving Party; (b) known to the receiving Party at the time of disclosure; (c) rightfully obtained by the receiving Party on a non-confidential basis from a third party; or (d) is independently developed by the receiving Party without use of the disclosing Party's disclosed non-public, confidential, or proprietary information.

23.5 The provisions of this Clause 23 apply during the Term of the Agreement and for a period of three (3) years following the expiration of the Agreement.

24 PUBLIC STATEMENTS

24.1 Supplier is allowed to name Customer as a client for reference purposes in its marketing efforts and may strictly for the purpose thereof use Customer's tradenames and logos.

25 VARIATION OF THE AGREEMENT

25.1 NO AMENDMENT TO OR MODIFICATION OF, OR RESCISSION OR DISCHARGE OF THE AGREEMENT IS EFFECTIVE UNLESS IT IS IN WRITING, IDENTIFIED AS AN AMENDMENT TO OR RESCISSION OR DISCHARGE OF THE AGREEMENT, AND SIGNED BY AN AUTHORIZED REPRESENTATIVE OF EACH PARTY. ANY ADDITIONAL OR CONFLICTING TERMS CONTAINED ON ANY CUSTOMER PURCHASE ORDER SHALL NOT BE BINDING UPON THE PARTIES AND SHALL BE INVALID, NULL, VOID, AND UNENFORCEABLE.

26 ASSIGNMENT

26.1 Supplier is entitled to assign its rights and obligations under the Agreement to a third-party without Customer's approval, however, Customer is not entitled to assign any of its rights under the Agreement.

27 COSTS

27.1 Each Party shall bear its own costs and expenses incurred in connection with the Agreement and the transactions contemplated herein, including, without limitation, all fees of its counsel and accountants.

28 GOVERNING LAW AND ARBITRATION

28.1 The validity, construction and performance of the Agreement and the legal relations among the parties to the Agreement shall be governed by and construed in accordance with the laws of the State of New York without giving effect to its conflict of law principles.

28.2 In the event of any controversy or dispute related to or arising out of the Agreement, THE PARTIES AGREE TO WAIVE THEIR RIGHTS, IF ANY, TO A JURY TRIAL AND PRE-TRIAL DISCOVERY.

28.3 Any dispute, claim, or controversy arising out of or relating to the Agreement, or the breach thereof, shall be settled by binding and confidential arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules, and the place of arbitration shall be in New York, New York.

28.4 The Parties agree that all arbitration shall be confidential.

28.5 Each Party shall bear an equal share of the arbitrators' and administrative fees of arbitration unless the arbitrator assigns fees to one Party.

Version: 27 June 2022

BUNKER PROCUREMENT PLATFORM

The following Product Terms apply to the Bunker Procurement Platform (ClearLynx Pro Platform).

Description of the Solution

The Bunker Procurement Platform enables bunker procurement optimisation by connecting buyers and sellers in an independent, market neutral platform. The Bunker Procurement Platform handles general bunker inquiry management from procurement to payment, including contracts, fuel tests and quality reporting and audit trails. Further, the Bunker Procurement Platform helps buyers match suppliers with ports, manage confirmations, amendments, claims, fuel tests, documentation and invoicing etc.

In general, the Bunker Procurement Platform allows Customer to do the tasks listed below on desktop as well as ClearLynx mobile app:

- Customize the program with their settings and frequently used trading partners and areas.
- Manage open inquiries (RFQs).
- Manage vessels, ports, suppliers, agents, labs, fuel tests and claims.
- Generate an inquiry (RFQ) to the suppliers in a port.
- Compare the offers received from the suppliers on dynamic trading screens
- Generate a stem confirmation between the buyer and the seller with the buyers and sellers' relevant clauses and notifications to interested third parties.
- Generate stem amendments and cancellations.
- Manage contract and spot purchases.
- Manage closed orders.
- Initiate, track and settle claims and other non-conformance items.
- Track order documentation.
- Track accounts payable.
- Contract Management.
- Provide full audit trail for all transactions
- Make reports on business statistics and price performance including:
    a. Buyer price performance
    b. Bunker supplier delivery quality performance
    c. Fuel test performance (specs met, Sulphur, CCAI, density, water, etc.)
    d. Claim statistics
    e. Fuel purchase statistical and trending reports
    f. Port and contract reports
    g. Accounting reports

Responsibilities & Resources:

For the purpose of the initial implementation and training Parties shall have the following responsibilities set out below.

Supplier Responsibilities:

- Project management, review & report to Customer progress
- Product deployment & configuration
- Data population, migration, management and
- Provide knowledge

Customer Responsibilities:

- Provide project leader with approval authority, who is responsible for issue resolution and reviewing and accepting plan deliverables or changes
- Provide timely access to Customer resource that has adequate understanding of Client's existing data, systems, and reporting
- Provide deployment data to Supplier

Technical requirements

Customer is responsible for delivery of data (see below) to Supplier or making the data readily available for processing by Supplier in CSV templates.

Data

Supplier requires the following data from Customer to deliver the Solutions and related Cloud Services:

- Agents
- Broker users
- Buying entities
- Contracts (if applicable)
- Labs and surveyors
- Ports
- Bunker suppliers
- Users
- Vessels
- Transactions (If loading historical information)

With regard to any contact information provided by Customer on individuals employed or associated with bunker suppliers and agents, Supplier will have a right to use such contact information at its own discretion and Supplier is entitled to make such information available to other customers in the Solution e.g., on the public list of bunker suppliers. If Customer does not want the contact information to be disclosed on the public list of bunker suppliers, Customer can choose to mark such individual as a "private" contact for Customer in the Solution, in which case, Supplier will not make such contact information available on the public list of bunker suppliers.

Transactions and interaction facilitated through the use of the Bunker Procurement Platform
Supplier disclaims all liability for the general or commercial terms of any and all transactions, or any liability resulting from a transaction facilitated in whole or in part through the use of the Bunker Procurement Platform. In no way will Supplier be held liable for any costs or damages associated with users of Customer interacting with counterparties whether added to the Bunker Procurement Platform by Customer (e.g., as a new supplier), or selected from the current list of counterparties on the Bunker Procurement Platform.

Supplier does not have possession, and will not take possession at any time, of anything listed or sold through the Bunker Procurement Platform, and is not involved in the actual transaction between the Customer and bunker suppliers and agents in respect of the sale and purchase of any goods or services or other items. For the avoidance of doubt, all contracts relating to such sales and purchases are made directly by the Customer on such terms and conditions as it may agree. This is expressly acknowledged and agreed by the Customer when using the Bunker Procurement Platform.

While Supplier will make commercially reasonable efforts to vet the parties on the Bunker Procurement Platform as legal entitties, it is Customer's full and absolute responsibility to vet the counterparties with whom it interacts and transacts. Customer is responsible for selecting and vetting credit worthiness, terms and conditions and other factors related to its transactions.

If and when Customer and a seller/bunker supplier or agent conclude a transaction, such parties will be responsible of ensuring that there is agreement on all aspects of the transaction. Supplier will take no responsibility for any errors or omissions to the contract to which Customer and the bunker supplier or agent have agreed.

Third party software or data
MandrillApp is used to host email-services and Sisense hosts reporting & business intelligence services.

Special conditions
No special conditions.

Version: 28 April 2022

ClearLynx Pricing & Analytics

The following Product Terms apply to the ClearLynx Pricing and Analytics product.

Description of the Solution

Real-time pricing for all key fuel grades. Analytics including real-time volatility, port arbitrage, momentum indicators, and interactive pricing map to support optimizing bunker purchasing decisions. Daily reporting of HSFO, VLSFO, & LSMGO, spreads between VLSFO/HSFO and VLSFO/LSMGO. Port template and supplier directories providing information on ports of supply, grades available, contact information.

Technical requirements

None, solution is web-based

Data

N/A

Third party software or data

N/A

Special conditions

Customers will be required to provide an accurate list of approved users for the Site and will receive discrete login and passwords for each of their users. Each customer is responsible for maintaining an up-to-date list of participants on the Site, and promptly advising ClearLynx of any changes to personnel for purposes of adding or removing users.

Customer is fully responsible for use of the Site by the Users, and for preventing unauthorized use of the ID and any Account, and will use its best efforts to prevent the same. Customers agree that their personnel will not share or publish their personal, discrete login and user ID credentials to others within or without their companies.

Version: 1 June 2022

SERVICE DESCRIPTION

Description of the Services

Subject to the Parties entering into an Order, Supplier can provide the following Services which are integrated into the Solutions:

Access to and use of the Solution

Supplier shall provide Customer with access to the Solutions (web- and mobile app based).

Supplier will provide Customer with all relevant login access to the Solutions.

Based on the access to the Solution, Customer is entitled to use the Solution in accordance with the Agreement and the Order.

Implementation and migration services

Supplier will provide the following implementation and migration services to Customer.

Supplier has a designated customer success manager and sale account manager for each customer at no cost to Customer. Supplier offers in software feedback for customers to share bugs, improvements or issues as per below.

Training:

Supplier will provide group trainings to Customer's operators as well as trainings to designated super users as reasonably necessary for the effective use of the Services. Depending on the type and quality of data Customer maintains, Supplier will make best efforts to migrate historical data into the software packages at a cost to be determined.

Normally, with any project deployment without customizations, implementation and training can occur within 30 days after contracts have been signed to allow time for system and data configuration. Any additional configurations determined during training may be able to be implemented into the system before go-live. Any requested customizations to be discussed for time cost and resources.

Go-Live services:
Supplier will perform set-up services, such as project management, design, development, implementation, integration, conversion, testing, installation, documentation and training services, as necessary.

Documentation
The documentation for any Solution will describe fully and accurately the features and functions of the Solution well enough to allow a reasonably skilled user to effectively use all of its features and functions without assistance from Supplier.

Operation and management of the Solution

Supplier will operate and manage the Solution, including the underlying technical infrastructure and software, in order to ensure its availability to Customer in accordance with the Agreement.

Supplier will continuously monitor the Solution for any technical, security, performance or other issues and take appropriate measures to address such issues, including diagnostics/troubleshooting, configuration management and system repair management.

The operation of the Solution also includes continuous updates of business continuity plans, contingency plans and disaster recovery plans on an ongoing basis.

Maintenance services

The Solutions and Services will regularly be improved, amended and enhanced to meet the business demands of the customer base and in accordance with the roadmap of Supplier. Supplier will update the Service Description accordingly.

Supplier will provide (i) regular scheduled maintenance tasks and activities and (ii) limited unplanned/emergency maintenance tasks and activities.

Support services

Customer will have access to Supplier's support services. Customer support is designated per customer. Each customer will be assigned a customer success manager. Support can be reached in three methods: (i) through an in-tool feedback button directly in a Solution, (ii) via email to Supplier's customer team at the email inserted below or (iii) by phone to Supplier's customer team to find Customer success managers contact details, phone number is inserted below.

Email: support@clearlyx.com

Telephone: +1 203 616 4333

Supplier will provide standard support between 8 AM and 7 PM EST, Monday through Friday, excluding US national holidays, as part of the Agreement.

Supplier will provide support services in accordance with industry practice. On-site support will be available to the extent specifically agreed with Supplier.

Material sub-suppliers

Sisense
Amazon Web Services ("AWS")

Please note that Supplier is entitled to change a material sub-supplier as set out in Suppliers T&Cs and/or any Product Terms.

Version 13 April 2022

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

ANNEX

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.

Clause 7

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 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 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) 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.

(e) 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.

(f) 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.

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): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

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): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: ClearLynx LLC

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

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

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

The 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 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 controller

The purpose of the processing is to registrer the employees of the 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 controller until the main agreement is terminated. If a user's employment ceased the controller may either delete or have the 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

Amazon Web Services, Inc.: 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 ClearLynx, LLC 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

- 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).

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

1. Name: Amazon Web Services, Inc.

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

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.

Sub-processors engaged by Amazon Web Services

Please see attached appendix.

11 July 2022

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 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 K.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 MENA FZ-LLC	United Arab Emirates
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 Amazon Simple Email Service Amazon Simple Notification Service Amazon WorkDocs	Seller and provider of the AWS services listed to the left for customers based in Japan
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 Lex Amazon Polly Amazon Rekognition Amazon Textract Amazon Transcribe Amazon Translate	USA	Service improvement

	Contact Lens for Amazon Connect		

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: June 9, 2022

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor

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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) 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 I.A. (hereinafter each "data exporter"), and

(ii) 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 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 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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(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:

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e)

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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 I.B.

Clause 7

Docking clause

(a) 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 I.A.

(b) Once it has completed the Appendix and signed Annex 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 I.A.

(c) 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

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be

fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into

another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement

Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State (as stated the Order): The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679 (as stated the Order): The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679 (as stated the Order): The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) 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.

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

(i) 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;

(ii) 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[4];

(iii) 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.

(c) 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.

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

(e) 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

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) 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. 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 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:

(i) 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

(ii) 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.

(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.).

(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 minimization

(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.

(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:

(i) 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;

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

(iii) 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 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) 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. 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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Denmark.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: Customer name is set out in the Order.

Address: Customer address 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 date: *Signed together with the Order.*

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.

Name: ClearLynx LCC

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

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

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

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

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.

The processor will not process sensitive data.

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

The data is transferred on a continuous basis.

Nature of the processing

The processor offers a web-based Bunker Platform which handles all aspects of inquiry management from procurement 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 controller and its employees are matched with suppliers or buyers at necessary ports. Further, the Platform manages confirmations, amendments, claims, fuel tests, documentation and invoicing.

Purpose(s) of the data transfer and further processing

The purpose of the processing is to registrer the employees of the 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.

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

The personal data is processed on behalf of the controller until the main agreement is terminated. If a user's employment ceased the controller may either delete or have the 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 transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Amazon Web Services, Inc.: 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 ClearLynx, LLC 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).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
The competent supervisory authority of the Customer is set out in the Order.

ANNEX II

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

- 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 III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

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

1.

Name: Amazon Web Services, Inc.

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

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

Description of 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
Please see attached appendix to the dpa.