tradesolution

DATA PROCESSING AGREEMENT

1. Background and purpose of the agreement

This Data Processing Agreement **("DPA")** is entered into between the customer (**"Data Controller"**) and Tradesolution AS (organization number 968 788 434) (**"Data Processor"**), jointly referred to as the **"Parties"**. The appendices attached to this DPA shall form an integral part of the DPA and its clauses.

The Data Processor collects, records, aligns, stores or in other ways processes Personal Data on behalf of the Data Controller in order to deliver the agreed-upon services in accordance with the Service Agreement ("the Service Agreement").

The purpose of this DPA is to:

a) regulate the Parties roles and responsibilities in relation to the processing of Personal Data pursuant to Data Protection Laws and the GDPR Article 28 (3) when fulfilling their duties according to the Service Agreement; and

b) ensure that the Data Subjects' Personal Data are not subject to unauthorized or unlawful processing.

The clauses of this DPA shall take priority over any similar provisions contained in any other agreements between the Parties. including the Service Agreement.

2. Definitions

The following definitions shall apply in relation to this DPA:

"**DPA**" shall mean the provisions and appendix' of this Data Processing Agreement.

"**Personal Data**" shall mean any information relating to a Data Subject. This includes, but is not limited to, the data described in Appendix 1 of this DPA.

"**Processing**" (of Personal Data) shall mean any use of Personal Data, such as, but not limited to, collection, storage, organization, alteration or adaption, distribution and/or transfer.

"**GDPR**" shall mean the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (as it is implemented into Norwegian law).

"**Data Protection Laws**" shall mean Act of 15 June 2018 no. 38 relating to the processing of personal data (The Norwegian Personal Data Act) and its appurtenant regulation and other legislation implementing the GDPR.

"Law" shall mean any other applicable legislation to which the Parties are subject.

"**Sub-Processor**" shall mean a Data Processor used by the Data Processor to Process Personal Data.

"**Data Subjects**" shall mean any identified or identifiable natural person.

3. General

The Parties shall process Personal Data in accordance with the Data Protection Laws, the GDPR and this DPA.

The Parties shall immediately notify each other if either Party is of the opinion that instructions or requirements from the other Party is in violation with the Data Protection Laws or the GDPR.

The Data Processor may process all the Personal Data necessary to deliver the agreed-upon services as well as administering the contractual relationship.

Appendix 1 sets out which Personal Data the Data Processor processes and the purpose of the processing. The Data Processor shall not process Personal Data for other purposes than those set out hereunder.

4. Rights and obligations of the Data Controller

The Data Controller shall determine the purposes and means of the processing of the Personal Data.

The Data Controller is responsible for ensuring that the Personal Data is processed in accordance with the Data Protection Laws and the GDPR.

The Data Controller shall, among other, ensure that it has a legal basis for the processing of the Personal Data.

The Data Controller shall have the right to terminate this DPA if the Data Processor does not comply with with the Data Protection Laws and the GDPR.

Unless otherwise is agreed or otherwise follows from the Law, The Data Controller shall be entitled to access the Personal Data that the Data Processor processes and the systems that the

Data Processor uses for processing purposes. The Data Processor shall provide necessary assistance if such access is required by the Data Controller.

5. Instructions to the Data Processor

The Data Processor shall only process Personal Data in accordance with documented instructions from the Data Controller, unless required to do so by Law to which the Data Processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Data Controller's instructions to the Data Processor are set out in this DPA and the appendices.

The Data Controller may give the Data Processor subsequent instructions throughout the duration of the Data Processor's processing of Personal Data on behalf of the Data Controller. Such subsequent instructions shall always be provided to the Data Processor in writing and must be documented.

6. Confidentiality

The Data Processor shall keep the Personal Data DPA confidential.

The Data Processor shall only grant access to the Personal Data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality by way of a non-disclosure agreement or who are under an appropriate statutory obligation of confidentiality and only on a need to know basis.

The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

7. Security of the processing

The Data Processor and the Data Controller shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with GDPR article 32, including inter alia as appropriate:

a) pseudonymisation and encryption of Personal Data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

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

The appropriate technical and organizational security required to achieve a level of safety appropriate to the risk are set out in Appendix 2.

The Data Processor shall make reasonable efforts to assist the Data Controller in ensuring compliance with the requirements for establishing an appropriate level of security in accordance with the GDPR Articles 35 – 36.

8. The Data Processor's use of Sub-Processors

The Data Processor shall meet the requirements specified in GDPR Article 28 (2) and (4) when engaging Sub-Processors.

The Data Processor has the Data Controller's general authorisation for the engagement of sub-processors.

The Data Processor shall inform the Data Controller in writing on their website, https://tradesolution.no of any intended changes concerning the addition or replacement of sub-processors at least two weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix 3. The list of sub-processors already authorised by the data controller can be found in Appendix 3.

If the Data Processor engages a Sub-processor for carrying out processing activities on behalf of the Data Controller, the same data protection obligations as set out in this DPA shall be imposed on that Sub-processor by way of a contract or other legal act.

9. The Data Processor's transfer of Personal Data to third countries and international organizations

The Data Processor may transfer and store Personal Data processed by the Data Processor on behalf of the Data Controller in countries where the Data Processor and its Sub-contractors' operates.

The Data Controller accepts such transfer and storage as long as it is necessary to complete the agreed deliveries.

The Data Processor can transfer Personal Data to a country or international organization outside the EEA without the prior written consent of the Data Controller. By transfer of Personal Data outside the EEA area or to an international organization, the Data Processor shall ensure that the requirements for the transfer of personal data to third countries or international organisations set out in GDPR chapter V are met.

An overview of our subcontractors from third countries can be found here:

https://tradesolution.no/personvern#1525352001021-7b51a261-b895 (our subcontractors)

10. Assistance to the Data Controller

The Data Controller shall act as the Data Subject's contact point and provide all necessary information regarding the processing.

The Data Controller is responsible for the handling of the Data Subjects requests for access, rectification, erasure, restriction, data portability etc., as well as ensuring that such requests are met.

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

If the Data Processor receives a request from any Data Subject, it shall as soon as possible notify the Data Controller.

11. The Parties' responsibility in relation to personal data breach management and notification

Any unauthorized processing of Personal Data in violation of GDPR article 32, the established routines of the Data Processor pursuant to GDPR article 32, instructions from the Data Controller or Data Protection Laws shall be handled as a personal data breach.

The Parties shall establish and maintain routines and systematic measures for the follow-up of personal data breaches, including measures for restoring normalcy, removing the cause for the breach as well as prevent repetition.

Once becoming aware of the deviation, inter alia a possible personal data breach, the Parties shall, without undue delay, notify the other party and immediately effectuate all necessary and appropriate measures to restore normalcy.

The Data Controller is responsible for notifying the Data Protection Authority and/or the Data Subjects in accordance with GDPR Article 33 and 34.

The Data Processor shall assist the Data Controller in in ensuring compliance with GDPR Article 33 and 34.

To assist the Data Controller in notifying the Data Protection Authority and/or the Data Subjects in accordance with GDPR Article 33 and 34, the Data Processor is required to assist the Data Controller in obtaining all necessary information needed to inform the Data Protection Authority and/or the Data Subjects in line with the requirements under GDPR Article 33 and 34.

12. Audits and inspections

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations under the Data Protection Laws, the GDPR and this DPA.

The Data Processor shall regularly audit the systems used to process Person Data. The audit may include review of routines, random controls and other appropriate measures.

If requested by the Data Controller the data processor shall, at the Data Controllers expense, allow for and make reasonable efforts to contribute to audits of the Data Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and this DPA by the Data Controller or an independent third party mandated by the Data Controller.

The Data Controller is entitled to request such audits once a year.

13. Term

This DPA shall remain in force as long as the Data Processor processes Personal Data on behalf of the Data Controller.

14. Termination

Upon termination of this DPA, the Data Processor shall erase all Personal Data comprised by this DPA unless applicable Laws requires storage of the Personal Data.

The Personal Data shall only be erased following written instructions from the Data Controller.

The Parties shall agree on how the transfer and/or erasure of the Personal Data shall take place.

The Data Processor shall document in writing that the personal data is erased without undue delay upon termination of this DPA.

15. Governing law and legal venue

This DPA shall be governed by and in accordance with the laws of Norway. Oslo District Court is the legal venue for any disputes between the Parties relating to this DPA.

***

Please return a signed copy of this DPA to Tradesolution AS by e-mail using the following e-mail address: regnskap@tradesolution.no. Please note that the agreement must be signed by a person authorized to sign on behalf of your company.

***

The Data Processor (Signature):	
Tradesolution AS	
Signature:	
Name & title:	Sigmund Berle Jensen, CEO

The document is electronically signed by customer on the last page.

Appendix 1 – Information about the Personal Data and the purpose of processing

The Purpose of the processing	Categories of Personal Data	Categories of Data Subjects	Duration of the processing
Performance of the services set out in the Service Agreement.	Contact information (mobile number, e-mail address, postal address etc.)	Customers of the Data Controller	For the duration of the Service Agreement
Performance of the services set out in the Service Agreement.	Personal information (name, age, position, gender etc.)	Customers of the Data Controller	For the duration of the Service Agreement

Appendix 2 - Description of technical and organizational measures

Use of cloud services:

We use Microsoft Azure and its security settings.

Authentication 1:

Two-factor authentication when guests (e.g. consultants).

Authentication 2:

No employee knows the password of our customer's users. This is handled in Azure.

Authorization:

Our admin portal (internal customer system) ensures that all customers and their users only have access to correct data and services.

Single Sign On (SSO):

If desired, we may offer SSO to all customers. This means that our customers can add and/or remove their own users` access to the services we provide.

Hardware (e.g. lap tops, phones and tablets):

All hardware is installed using a system that monitors compliance with the correct security policy. (password/PIN, VPN-tunnels, e-mail storage and document management.).

Internal IT Policy:

All our employees are obliged to read, understand and sign a non-disclosure agreement and our IT-policy. Our IT policy shall be updated regularly. Our employees must re-sign our agreement each year.

Logging and monitoring of services:

We continuously monitor and log activity at both the service and at the user level in order to maintain the integrity of our systems and services.

Back-up and disaster recovery

We have sufficient back-up routines and carry out disaster recovery training regularly.

Appendix 3 - Overview of the Data Processor's Sub-contractors

Company	Registration no.	Address	Contact details	Processing and storage locations (country/state)
Microsoft Ireland Operation LTD	IE8256796U	Sandyford Business-Estate 1885008, Dublin D 18, IRLAND		Nederland (Azure) Back-up in Ireland
Lime Technologies Norway AS	989 711 393	Inkognitogata 33, 0256 Oslo, Norway	Info.no@lime.tech	Ireland (Amazon)
Nitschke & Borgting AS	962 077 447	Henrik- Ibsensgate 60A 0255 OSLO 8001 Bodø, Norway	+ 47 22 94 25 50	Nederland (Azure). Back-up in Ireland. Store-and-forward operation – servers in Bodø and Trondheim.
Coretrek AS	984 587 406	Nordre Kullerød 1 3241 SANDEFJORD	Info@coretrek.no	Back up in Norway
Lindorff AS	835 302 202	PB. 7055 3007 Drammen, Norway	+ 47 23 21 10 00	Finland (Fujitsu
Evry Norge AS	933 012 867	Snarøyveien 30A, 1360 Fornebu, Norway	+ 47 23 14 50 00	Processing within the EU/EEA
Logrocket		87 Summer St. Boston, MA 02110	https://logrocket.com/contact/	USA
Beamer		Boulder, Colorado	info@getbeamer.com	USA
Google Cloud		1600 Amphitheatre Parkway Mountain View, CA 94043	https://cloud.google.com/contact	USA
Amazon Web Services		410 Terry Avenue North Seattle, WA 98109	1-206-266-1000	USA
Intercom		55 2nd Street, 4th Floor,San Francisco, CA 94105	https://www.intercom.com/ Chat	USA
Statuspage		Sydney, AU	https://support.atlassian.com/statuspage/	USA