DataEquipment

Data Processing Agreement

Data Processing Agreement

between

[the Customer]
(the "**Data Controller**")

and

Data Equipment AS
(the "**Data Processor**")

(each referred to as a "**Party**", and collectively, the "**Parties**")

[DATE]

1 DEFINITIONS

The Agreement	This data processor agreement.
The Main Agreement	The agreement and General Terms and Conditions entered into between the Data Controller and the Data Processor for provision of the Intellisec Managed Services or Products and Consultancy Services which form the basis for the processing of personal data.
The Data Controller	The natural or legal person which alone or in cooperation with others decides the purpose of the processing of personal data i accordance with this Agreement: T**he Customer as specified in the Main Agreement.**
Personal Data	Any information regarding an identified or identifiable private individual which is processed by the Data Processor on behalf of the Data Controller.
The Data Processor	The natural or legal person processing personal data on behalf of the Data Controller in accordance this Agreement: **Data Equipment AS.**

2 PURPOSE

The Agreement and its clauses (the Clauses) set out the rights and obligations of the data controller and the data processor when the data processor processes personal data on behalf of the data controller.

These Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing of Directive 95/46/EC (General Data Protection Regulation).

In the context of the Data Processor's provision of the agreed products or services pursuant to the Service Agreement, the data processor will process personal data on behalf of the Data Controller in accordance with these Clauses. The Parties agree that the data processor shall process personal data on behalf of the data controller for the sole purpose of carrying out the tasks assigned to the data processor by the data controller when providing the agreed products or services.

The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

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

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

Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
Appendix C contains the data controller's instructions for the data processor's processing of personal data, a description of the minimum security measures to be implemented by the data processor, and how audits of the data processor and any sub-processors shall be carried out.

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

These Clauses shall not exempt the data processor and the data controller from obligations to which the data processor and data controller are subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation

3 THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 of the GDPR), the applicable EU or Member State[1] data protection provisions and these Clauses.

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

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

4 THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

The data processor, and any person acting on behalf of the data processor with access to personal data, shall only process personal data on documented instructions from the data controller. The parties agree that the provisions of this Agreement and the Service Agreement or Agreement shall be construed as such instructions from the Data Controller. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, with the Clauses.

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

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

5 CONFIDENTIALITY

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 or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible to those persons. The data processor shall at the request of the data controller be able to demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6 SECURITY OF PROCESSING

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

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

a) pseudonymisation and encryption of personal data;

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

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

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

According to Article 32 of the GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 of the GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 of the GDPR along with all other information necessary for the data controller to comply with the data controller's obligation un-der Article 32 of the GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented, than those already implemented by the data processor, the data controller shall specify these additional measures to be implemented in Appendix C.

7 USE OF SUB-PROCESSORS

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

The data processor shall therefore not engage a sub-processor for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

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 of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the sub-processor(s) in question. Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in these Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.

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

A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in these Clauses are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8 TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

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

In case a transfer to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

Without documented instructions from the data controller, the data processor therefore cannot within the framework of these Clauses:

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

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

c) process the personal data in a third country

The data processor is hereby mandated by the data controller to transfer personal data to its affiliates located in a country outside of the EEA or the EU, and to allow such affiliate to access and process personal data solely for the purposes stated in Appendix A. The data processor warrants that such transfer is in accordance with the GDPR and will upon request provide the data controller with signed Standard Contractual Clauses or other document evidencing compliance with these Clauses and the GDPR.

These Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) of the GDPR, and these Clauses cannot be viewed as basis for transfer of personal data under Chapter V of the GDPR.

9 ASSISTANCE TO THE DATA CONTROLLER

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 possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

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

a) the right to be informed when collecting personal data from the data subject

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

c) the right of access by the data subject

d) the right to rectification

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

f) the right to restriction of processing

g) notification obligation regarding rectification or erasure of personal data or restriction of processing

h) the right to data portability

i) the right to object

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

In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a) the data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify any personal data breach to the Norwegian data protection authority (Nw "Datatilsynet") unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b) the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c) the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d) the data controller's obligation to consult the Norwegian data protection authority (Nw "Datatilsynet") prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

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

10 NOTIFICATION OF PERSONAL DATA BREACH

In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data

controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the GDPR.

In accordance with clause 9(2)(a) of these Clauses, the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) of the GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

b) the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11 ERASURE AND RETURN OF DATA

On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12 AUDIT AND INSPECTION

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

Should the data controller request an audit of the data processor in addition to the compliance information provided, the controller shall bear both parties' costs incurred as a result of the audit. The data processor shall bill for the accrued time, based on the hourly rate stated in the contract with the data controller. Notwithstanding the foregoing, if the audit or inspection reveals that the data processor has not complied with its obligations under these Clauses or the GDPR, the data processor shall bear all reasonable costs.

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

13 COMPENSATION AND LIABILITY

Each party shall be liable for claims, costs, loss, fines, expenses or damages incurred by the other party as a result of the party's breach of this Agreement, including non-compliance with the GDPR. The limitation of liability of the Main Agreement shall apply correspondingly, apart from liability pursuant to Article 82 of the GDPR**.**

14 COMMENCEMENT AND TERMINATION

The Agreement shall apply for as long as the data processor processes personal data on behalf of the data controller, and the Agreement is subject to the same rules for termination as stipulated in the Main Agreement. If the Main Agreement expires or is terminated, the Agreement shall lapse correspondingly.

15 DATA CONTROLLER AND DATA PROCESSOR'S CONTACT POINTS

Notifications pursuant to this Agreement shall be submitted in writing to the Parties' designated contact points as stated in the Main Agreement.

The parties shall be under obligation to continuously inform each other of changes to contacts/contact points under this Agreement and the Main Agreement.

APPENDIX A – INFORMATION ABOUT THE PROCESSING

Information about the personal data processed by the data processor:

Personal name	X	☐
Contact information (Address, e-mail, phone number, etc.)	X	☐
Reference number / Customer number / Employee number	X	☐
Information of next of kin		☐
Information about children		☐
National identity number / Social security number		☐
Employment information	X	☐
Information on customer relationship	X	☐
Details of insurance		☐
Financial information	X	☐
Medical or health information		☐
Genetic data		☐
Biometric data		☐
Information about sexual relationships		☐
Information relating to litigation and criminal offenses		☐
Information on racial or ethnic background		☐
Information on political, philosophical or religious beliefs		☐
Information on union membership		☐

Comments / categories beyond the above	
Purposes	The purpose of the processing is to provide security services to the data controller in accordance with the Main Agreement.
Categories of data subjects	• The data controller's employees • The data controller's customers • The data controller's suppliers
Retention time	The duration of the customer relationship

APPENDIX B – SUB-PROCESSORS

B.1. Approved sub-processors

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

NAME	CVR.	ADDRESS	DESCRIPTION OF THE PROCESSING
Duo Security LLC		123 North Ashley Street, Suite #200, Ann Arbor, MI 4810	Provides multi-factor authentication. More information on the data processing can be found here.
Tenable Network Security Ireland Limited	IE572635	81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland	Provides "Vulnerability scanning as a service". More information on the data processing can be found here.
Palo Alto Networks		3000 Tannery Way Santa Clara, CA 95054	Provides "Managed Firewall". More information on the data processing can be foundhere.
Proofpoint LTD		100 Brook Drive, Green Park Reading, Berkshire RG2 6UJ	Provides "Managed Email Protection". More information on the data processing can be found here.
Google Cloud		1600 Amphitheatre Parkway Mountain View, CA 94043	Delivers Compute and infrastructure services. More information on the data processing can be found here.
Elastic		Keizersgracht 281 1016 ED Amsterdam	Delivers database services. More information on the data processing can be found here.
Auth0 docs			Delivers authentication and logins. More

NAME	CVR.	ADDRESS	DESCRIPTION OF THE PROCESSING
			information on the data processing can be found here.
Atlassian (Jira)		Sydney (Global HQ) Level 6, 341 George Street, Sydney, NSW 2000, Australia.	Delivers support system. More information on the data processing can be found here.
Egnyte		1350 W. Middlefield Road Mountain View, CA 94043.	Delivers system for file storage. More information on the data processing can be found here.
Extreme Cloud IQ		San Jose, CA 6480 Via Del Oro San Jose, CA 95119.	Delivers managementsystems for "network as a service" and management interface. More information on the data processing can be found here.

At commencement of the Clauses, the data controller has approved using the above-mentioned sub-processors for the processing described for each respectively. The data processor cannot, without the data controller's explicit written approval, use a sub-processor for any other processing activity than what is pre-agreed for the specific sub-processor, or use another sub-processor for the processing activity in question.

APPENDIX C – THE DATA PROCESSOR'S GENERAL PROCESSING SECURITY MEASURES

The data processor guarantees that the appropriate technical and organisational security measures are in place at all times in order to ensure that personal data is protect-ed against illegal or accidental destruction, loss, damage, alterations, and unauthorised access. This particularly applies where the processing involves online transfer of data and all other illegal transfer of data.

Such technical and organisational security measures include but are not limited to: Encryption of customer data with TLS or similar during transfer, multi-factor authentication in the systems that are used for storage or management of customer data, as well as implementation of least privilege and zero trust safety modules throughout the organisation as well as towards all processors and handlers of data.

All systems for the storage, transportation and processing of customer data happens in accordance with Data Equipment's security policy, available here.