1. PURPOSE OF THIS DATA PROCESSING AGREEMENT

1 This Agreement (the "Data Processing Agreement") sets out the Parties' rights and obligations when the Data Processor processes personal data on behalf of the Data Controller, as part of the services delivered under the agreement entered into between Tribia AS or Tribia AB and Customer (the "Main Agreement").This Data Processing Agreement is entered into and accepted as part of the Main Agreement.This Data Processing Agreement is based on the Norwegian States Standard Data Processing Agreement available on https://www.anskaffelser.no/verktoy/kontrakterogavtaler/databehandleravtaleogsjekkliste and is an integrated part of the Main Agreement.The purpose of the Data Processing Agreement is to ensure that the Parties comply with the Applicable Privacy Policy.The Data Processing Agreement comprises this document, as well as Appendices A, B, C and D.

1 In the event of conflict between the terms of the Main Agreement and the Data Processing Agreement, the terms of the Data Processing Agreement will take precedence regarding matters specifically related to the processing of personal data. In the event of any conflict between the Data Processing Agreement and its Appendices, the Appendices will take precedence.

1 Appendix A of The Data Processing Agreement includes a detailed description of the processing that is to take place, as well as the purpose of processing, categories of personal data and data subjects. The Parties' designated contact persons are specified in the Main Agreement.

1 Appendix B of The Data Processing Agreement includes conditions for the use of Subprocessors, as well as a list of approved Subprocessors.

1 Appendix C of the Data Processing Agreement contains specific instructions for the processing of personal data under the Main Agreement, including security measures and the Data Controller's right of access to and audit of the Data Processor and any Subprocessors, as well as sectorspecific provisions concerning the processing of personal data.

1 Appendix D of the Data Processing Agreement contains changes to the standard text and any subsequently agreed changes to the Data Processing Agreement.

2. DEFINITIONS

Applicable Privacy Policy: The applicable versions of the EU's General Data Protection Regulation (2016/679) ("GDPR") and the Norwegian Act on the Processing of Personal Data of 15.06.2018 (the Personal Data Act) with related regulations etc., and any other relevant legislation concerning the processing and protection of

Main Agreement: One or more agreements between the Data Controller and the Data Processor concerning the provision of services which entail the processing of personal data, as specified in Appendix A. The Data Processing Agreement

Subprocessor: A company or person used by the Data Processor as a subcontractor for the processing of personal data under the Main Agree-

Article 4 of GDPR will apply to privacy policy terms not defined in this

3. RIGHTS AND OBLIGATIONS OF THE DATA CON-

The Data Controller is responsible for the processing of personal data in accordance with the Applicable Privacy Policy. The Data Controller must spe-

i. the processing of personal data is for a specified and explicit purpose and is based on valid legal grounds

ii. the data subjects have received the necessary information concerning the processing of the personal data

iii. the Data Controller has carried out adequate risk assessments; and

iv. the Data Processor has at all times, adequate instructions and information to fulfil its obligations under the Data Processing Agreement and the Applicable Privacy Policy.

4. INSTRUCTIONS FROM THE DATA CONTROLLER TO THE DATA PROCESSOR

4 The Data Processor shall process the personal data in accordance with the Applicable Privacy Policy and the Data Controller's documented instructions, cf. section 4.2. If other processing is necessary to fulfil obligations to which the Data Processor is subject under applicable law, the Data Processor must notify the Data Controller to the extent this is permitted by law, cf. Article 28 (3) (a) of GDPR.

4 The Data Controller's instructions are stated in the Data Processing Agreement with Appendices. The Data Processor must notify the Data Controller immediately if the Data Processor believes the instructions conflict with the Applicable Privacy Policy, cf. Article 28 (3) (h) of GDPR.

4 The Data Processor must be notified in writing of any requested changes to the instructions in the Data Processing Agreement with Appendices, and changes must be implemented by the Data Processor by the date agreed between the Parties or. The Data Processor may require the Data Controller to pay documented costs accrued in connection with the implementation of such changes, or the proportional adjustment of the remuneration under the Main Agreement if the amended instructions entail additional costs for the Data Processor. The same applies to additional costs that accrue due to changes in the Applicable Privacy Policy which concern the activities of the Data Controller.

5. CONFIDENTIALITY AND DUTY OF SECRECY

5 The Data Processor must ensure that employees and other parties who have access to personal data are authorised to process personal data on behalf of the Data Processor. If such authorisation expires or is withdrawn, access to the personal data must cease without undue delay.

5 The Data Processor must ensure that persons authorised to process personal data on behalf of the Data Controller are subject to obligations of confidentiality either by agreement or applicable law. The obligations of confidentiality shall survive the duration of the Data Processing Agreement and/or employment relationship.

5 At the request of the Data Controller, the Data Processor shall document that the relevant persons are subject to said obligations of confidentiality see section 5.3.

5 Upon the expiry of the Data Processing Agreement, the Data Processor is required to discontinue all access to personal data that is processed under the agreement.

6. ASSISTANCE TO THE DATA CONTROLLER

6 When requested, the Data Processor shall as reasonably requested assist the Data Controller with the fulfilment of the rights of the data subjects under Chapter III of the GDPR through appropriate technical or organisational measures. The obligation to assist the Data Controller solely applies insofar as this is possible and appropriate, taking into consideration the nature and extent of the processing of personal data under the Main Agreement.

6 Without undue delay, the Data Processor shall forward all enquiries that the Data Processor may receive from the data subject concerning the rights of said data subject under the Applicable Privacy Policy to the Data Controller. Such enquiries may only be answered by the Data Processor when this has been approved in writing by the Data Controller.

6 The Data Processor must assist the Data Controller as reasonably requested in ensuring compliance with the obligations pursuant to Articles 3236 of GDPR, including providing assistance with personal data impact assessments and prior consultations with the Data Protection Authorities, in view of the nature and extent of the processing of personal data under the Main Agreement.

6 If the Data Processor, at the reasonable request of the Data Controller, provides assistance as described in sections 6.1 or 6.3, and the assistance goes beyond what is necessary for the Data Processor to fulfil its own obligations under the Applicable Privacy Policy, the Data Processor will be reimbursed in accordance with the price provisions of the Main Agreement.

7. SECURITY OF PROCESSING

7 The Data Processor shall implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Data Processor must, as a minimum, apply the measures specified in Appendix C of the Data Processing Agreement.

7 The Data Processor shall carry out risk assessments to ensure that an ap-

8. NOTIFICATION OF BREACH OF PERSONAL DATA

8 In case of a personal data breach, the Data Processor shall without undue delay, notify the Data Controller in writing of the breach, and in addition provide the assistance and information necessary for the Data Controller to be able to report the breach to the supervisory authorities in line with the Applicable Privacy Policy.

8 Notification in accordance with section 8 must be given to the Data Controller's point of contact specified in the Main Agreement, and must:

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories of and approximate number of personal data records concerned

b. state the name and contact details of the data protection officer or other contact point from where more information can be obtained

c. describe the likely consequences of the personal data breach; and

d. describe the measures taken or proposed by the Data Controller to address the breach, including where appropriate, measures to mitigate possible adverse effects.

If necessary, information may be given in phases without any further undue delay.

8 The Data Processor shall implement all necessary measures that may reasonably be required to rectify and avoid similar personal data breaches. As far as possible, the Data Processor must consult the Data Controller concerning the measures to be taken, including assessment of any measures proposed by the Data Controller.

8 The Data Controller is responsible for notifying the Data Protection Authority and the data subjects affected by the personal data breach. The Data Processor may not inform third parties of any breach of personal data security unless otherwise required under applicable law or in accordance with the express written instructions of the Data Controller.

9. USE OF SUBPROCESSOR

9 The Data Processor may only use Subprocessors with the prior general or specific written authorisation of the Data Controller, in accordance with Appendix B of the Data Processing Agreement. For an overview of approved Subprocessors, see Appendix B of the Data Processing Agreement.

9 If a Data Processor engages a Subprocessor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the Subprocessor by way of written agreement. See section 9.7 concerning the use of standard thirdparty services.

9 The Data Processor may only engage Subprocessors who provide appropriate technical and organisational measures to ensure that the processing fulfils the requirements in accordance with the Applicable Privacy Policy. The

Data Processor must use reasonable efforts to assess and verify that satisfactory measures have been taken by the Subprocessors. Upon request, the Data Processor must be able to submit reports from such assessments to the Data Controller.

9 If the Subprocessor fails to fulfil its data protection obligations, the Data Processor shall remain liable to the Data Controller for the performance of the Subprocessor's obligations in the same way as if the Data Processor himself was responsible for the processing.

9 The Data Processor is obligated, on request, to disclose agreements with Subprocessors to the Data Controller. This solely applies to the parts of the agreement that are relevant to the processing of personal data, and subject to any statutory or regulatory limitations. Commercial terms and conditions are not required to be submitted.

9 If the Data processor uses a subcontractor that provides standardised thirdparty services, the Parties may agree that the subcontractor's standard data processing agreement will be used and applied directly to the Data Controller as in a direct data processing relationship (i.e. not as a Subprocessor) under the following terms:

- The Data Controller must expressly accept under the Main Agreement that the standardised thirdparty services are provided on the subcontractor's standard terms
- The Data processor must follow up on the standard terms on behalf of the

10. TRANSFER OF PERSONAL DATA TO COUNTRIES OUTSIDE

10.1 Personal data may only be transferred to a country outside the EEA ('Third country') or to an international organisation if the Data Controller has approved such transfer in writing and the terms in section 10.3 are fulfilled. Transfer includes, but is not limited to:

a) processing of personal data in data centres, etc. located in a Third Country, or by personnel located in a Third Country (by remote access)

b) assigning the processing of personal data to a Subprocessor in a Third State; or

c) disclosing the personal data to a Data Controller in a Third Country, or in an international organisation.

10.2 1 The Data Processor may nonetheless transfer personal data if this is required by applicable law in the EEA area. In such cases, the Data Processor must notify the Data Controller, to the extent permitted by law.

10.3 1 Transfer to Third Countries or international organisations may only take place if there are the necessary guarantees of an adequate level of data protection in accordance with the Applicable Privacy Policy. Unless otherwise agreed between the Parties, such transfer may only take place on the fol-

a) a Data Processing Agreement which incorporates standard personal data protection provisions as specified in Article 46 (2) (c) or (d) of the GDPR (EU model clauses); or

c) binding corporate rules in accordance with Article 47 of GDPR.

10.4 Any approval by the Data Controller for the transfer of personal data to a Third Country or international organisation must be stated in Appendix B of the Data Processing Agreement.

11.1

11. AUDIT

11.2 Upon reasonable request, the Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this Data Processing Agreement.

11.3 The Data Processor shall allow and contribute to annual inspections and audits carried out by or on behalf of the Data Controller. The Data Processor shall also allow and contribute to inspections conducted by relevant supervisory authorities. The Data Controller's review of any Subprocessor shall be conducted by the Data Processor, if so specifically requested and agreed.

11.4 If an audit reveals a breach in the obligations in the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor must rectify the breach as soon as possible. The Data Controller may require the Data Processor to temporarily stop all or part of the processing activities until the breach has been rectified and approved by the Data Controller.

12.1 Each Party shall pay its own costs associated with an annual audit. If an audit reveals significant breaches of the obligations under the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor shall pay for the Data Controller's reasonable costs accrued from the audit.

12. ERASURE AND RETURN OF INFORMATION

12.2 Upon the expiry of this Data Processing Agreement, the Data Processor is obligated to return and erase all personal data processed on behalf of the Data Controller under the Data Processing Agreement, in accordance with the provisions of Appendix C. This also applies to any backup copies.

12.3 The Data Controller will determine how any return of personal data is to take place. The Data Controller may require return to take place in a structured and commonly used machinereadable format. The Data Controller will pay the Data Processor's documented costs associated with the return unless this is included in the remuneration under the Main Agreement.

12.4

12.5 If a shared infrastructure or backup is used and direct erasure is not technically possible, the Data Processor must ensure that the personal data is made inaccessible until it has been overwritten.

13.1 The Data Processor must confirm in writing to the Data Controller that the data has been erased or made inaccessible, and shall, upon request document how this has taken place.

13.2 If the Data Processor fails to comply with its obligations pursuant to this Data Processing Agreement and/or Applicable Privacy Policy, this shall be deemed a breach of the Main Agreement, and the obligations, deadlines, sanctions and limitations of liability in the Main Agreement's regulation of the Supplier's breach will be applied.

14. DURATION AND EXPIRY

14.1

1 The Data Processing Agreement will come into effect from the date it is signed by both Parties. The Data Processing Agreement shall apply for as long as the Data Processor processes personal data on behalf of the Data Controller. It shall also apply to any personal data held by the Data Processor or
14.2 any of its Subprocessors after the expiry of the Main Agreement.

1 The rules concerning termination specified in the Main Agreement shall also apply to the Data Processing Agreement, to the extent this is applicable. The Data Processing Agreement may not be terminated if the Main Agreement is in effect, unless it is replaced by a new Data Processing Agreement.

15. NOTIFICATIONS

Notification under this Data Processing Agreement shall be submitted in writing to: For Customer as Data Controller:

For Tribia as Data Proces-

Email to: GDPR@tribia.

16. GOVERNING LAW AND LEGAL VENUE

The Data Processing Agreement is governed by Norwegian law if the Data Controller is a Norwegian legal entity and by Swedish law if the Data Controller is a Swedish legal entity. Disputes will be resolved in accordance with the provisions of the Main Agreement, including any provisions concerning legal venue.

APPENDIX A

Purpose and instructi-

Tribia AS provides online collaboration project services ("Service") to Customer pursuant to the Main Agreement.

Personal data processed in the

In the Service, every user of the system is linked to a personal user profile. To be allowed to create a user profile, you must register the following compulsory

- First name
- Surname

The registered email address that is linked to a user is the unique username of that member and is used to log in to the system together with a password set by the user. Without this username and password, the member will not, under any circumstances, have access to and be able to log in to or get information from

Voluntary personal

Every user can register the following voluntary data in his or her own

- Picture
- Title
- Company
- Te-

All the data mentioned above is available as information for all users of the Service within each specific customer area.

Complimentary user information for support and security

- IP Address
- Computer Name

The Data Processor shall not process Personal Data beyond the requirements necessary to comply with the obligations under the Agreement without prior written agreement or written instructions from the Data Controller.

APPENDIX B

Subprocessors

The Data Processor engage following Subprocessors who provide appropriate technical and organisational measures to ensure that the processing fulfils the requirements in

Company	Address & Location	Processing region	Purpose
Orange Business	Nydalen Allè 37A 0484 Oslo Norway	Norway Sweden	Managed service for operations platform (server, network, security)
Auth0 Inc	3rd Floor Union House 182194 Union Street London, SE1 0LH, UK, LONDON	Germany/EU	Auth0 is an authentication and authorization platform (platformasaservice).
Microsoft	Dronning Eufemias gate 71, 0194 Oslo	Norway / EU	Operations platform (Microsoft Azure)
Truesec AB	Oxtorgsgränd 2, 111 57 Stockholm, Sverige	Sweden / EU	SOC service (Security Operations Center)

APPENDIX C

Security and instructi-

GENERAL

The Data Processor shall take all measures necessary under Article 32 of the Regulation, including planned, systematic, organizational and technical measures, ensuring adequate confidentiality, integrity, and availability of information in the processing of Personal Data. With reference to the technical and organisational measures specified in this section, the Supplier provides the following measures:

- Protection relating to physical access and logical access
- Multifactor authentication for admin purposes

ENCRYPTION OF

All data traffic and credentials are encrypted using TLS (Transport Layer Security) to ensure that no unauthorized access to data.

Data at rest (storage) is encrypted using AES 256 bit encryption and FIPS2

USER IDENTIFICATION

Users are identified by a valid combination of username and password. Authentication is managed with either SSO or builtin user repository. For password encryption, a oneway encryption is run and the password is never visible to any Tribia employees. By login a mechanism is run to prevent bruteforce attacks on

ACCESS

Users can access per project room and can for example have write permissions in a project, but only read rights in another. In addition, the read and write permissions can be set on all levels. Rights can be set based on individuals or

SAFETY TESTS AND SE-

Independent safety tests are done by expert communities to ensure against attacks such as crosssite request forgery (CSRF), crosssite scripting (XSS), SQL injections among other on technical level. Security is a continuous focus and

BASEFARM HOSTING

THE OPERATING ENVIRON-

There is great emphasis on the safety of the operating environment which is based in Norway and established at our professional operation partner Basefarm (hereafter The Operating Partner). The physical environment is divided into two data centers and information that is stored in the Solution is mirrored in real time

The datacenters are facilitated with access control, video surveillance, climate control, fire detection with early warning, emergency power and anything else that characterizes a modern and secure data center.

The operating environment are located in anonymous industrial buildings. Logos or other effects associated with our operating partner does not exist at the building. The terrain around is shaped so that there is little danger of flooding, and the buildings are solid. The risk of burglary is considered as small.

The buildings are located behind several massive steel doors that are connected to an alarm system that is monitored 24 hours a day through the

Access to the data centres is given only to personnel with special needs and when required with prior approval. Access Cards and code is also required at all times. Service technicians and any other personnel granted access only

All employees of our operating partner sign a standard confidentiality agreement. This also includes any access to customer data. Our operating partner staff have limited access / rights / access to customer data depends on users / user groups, which in turn is determined by the function they provide.

The data centre is monitored 24 hours a day, 365 days a year, through the Operating Partner`s support team. In the support team, there are always highly trained and qualified staff with extensive experience in the areas of

Connection to the Internet is robust and consists of redundant connection to the NIX and redundant connections to different providers for general Internet traffic. In addition, we have redundant interconnection against some major

Our Operating Partner has a quality system based on ISO. The processes involved in service delivery is in general based on ITIL.

FIREWALL

The Solutions platform is implemented behind redundant firewall service and loadbalancing from reputable suppliers. It is implemented unique rules for the firewall and policies based on the security requirements the Solution demands. The Operating Partner is responsible for all operation, maintenance and moni-

BACKUP & RESTORE

Backup service for the Solution consists of an advanced twolayer architecture with backup to disk and then to the underlying tape or disk storage in a third datacentre. This architecture leads to significantly shorter backup and restore

We have the following standard bac-

- Incremental backup is performed twice daily (at. 12:00 and 24:00)
- Deleted / changed files stored on backup for 30 days (retention)

Backup is taken daily in our Operating Partner's backup windows, with guaranteed response to restore in the event of hardware failure or data loss. Backup services are online and do not imply downtime for backup. Only authorized per-

Involved technicians must sign a declaration of confi-

MICROSOFT AZURE CLOUD

Azure Cloud Services offers a rich service catalog and a dynamic allocation of resources. In cooperation with our professional operation partner Basefarm, Azure is utilized to provide a stable and future proof operating environment for our applications and

THE OPERATING ENVIRON-

Azure Norway is used to ensure that all customer data stay located in Norway. In all Azure datacenters physical access to the areas where data is stored is strictly controlled. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. Cameras are located around the datacenters, with a security team monitoring their videos at all times. Professionally trained security officers also routinely patrol the data-

Controlled access points are located at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Physical access to the datacenter is strictly controlled and must be requested and approved before arriving at the datacenter. Permissions are granted on a needtoaccess basis and limited to a certain

Physical security reviews of the facilities are conducted pe-

The Azure infrastructure meets a broad set of international and industryspecific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

FIREWALL

The Azure platform Firewall is a managed, cloudbased network security service that protects our Network resources. It's a fully stateful firewall as a service with builtin high availability and unrestricted cloud scalability.

The Operating Partner in cooperation with Microsoft Azure is responsible for all operation, maintenance and monitoring of firewalls.

BACKUP & RESTORE

Backup service for the Solution running on Azure uses reliable Blob storage with inbuilt security and high availability features. When applicable, snapshots are used for some workloads such as VMs and Azure Files, drastically reducing the time to recover your

We have the following standard bac-

- Incremental backup is performed twice daily (at. 12:00 and 24:00)
- Deleted / changed files stored on backup for 30 days (retention)

Backup is taken daily with guaranteed response to restore in the event of hardware failure or data loss. Backup services are online and do not imply downtime for backup Access to backups is restricted only to authorized Backup Admins.

All infrastructure is represented as code and can quickly be rebuilt from scratch in case of a disastrous loss of data. Infrastructure code is located in a secure git repository. Infrastructure as code makes it easy to move the entire deployment of services to a diffe-

APPENDIX D

Agreed changes

The Parties agree to add the following wording in addition to what is stated

9.1 "The Data Controller hereby grants the Data Processor with a general authorization to engage Subprocessors".

The Parties agree to replace the provision in section 9.4 with the fol-

9 "The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of Subprocessors, thereby giving the Data Controller the opportunity to object to such changes. Such objection shall be made in writing and within thirty (30) calendar days after the Data Processor has informed the Data Controller about the intended changes. If the Data Controller objects to changes in the use of Subprocessors, the Data Controller may, as a sole remedy, terminate the Main Agre-

The Parties agree to replace the provision in section 11.2 with the fol-

11.2 1 The Data Processor shall upon prior reasonable notice allow and contribute to annual inspections and audits carried out by or on behalf of the Data Controller one time per calendar year. The Data Processor shall also allow and contribute to inspections conducted by relevant supervisory