Data Processing Agreement

This Data Processing Agreement ("**DPA**") is entered into between:

(A) [*name of customer*] of [*insert address*] ("**Customer**"); and

(B) [No Isolation Ltd] of [*insert address*] OR [No Isolation AS of Trondheimsveien 2, 0560 Oslo, Norway with registration number 815 716 272] ("**Supplier**").

Each a "**party**" and together the "**parties**".

1. **Incorporation of DPA into Agreement –** The parties have entered into an agreement for the purchase of certain products and services, including AV1 or Komp solutions ("**Agreement**"). In the performance of the Agreement, Supplier shall process certain Personal Data (as defined below) on behalf of Customer and this DPA shall apply to such processing. This DPA is hereby incorporated by reference into and shall form part of the Agreement. All terms in the Agreement shall remain in full force and effect except to the extent this DPA expressly modifies or conflicts with any such terms, in which case this DPA shall take precedence.

2. **Permitted Third Parties** – Customer may, subject to the terms of the Agreement and this DPA, allow a Permitted Third Party (based in the markets in which Supplier operates) to use the Services on condition that:

   (a) Customer notifies Supplier in writing of the identity of the Permitted Third Party (including name, address, contact details and details of the Services that will be used) before allowing the Permitted Third Party's use of the Service; and

   (b) the Permitted Third Party, Customer and Supplier jointly agree in writing to let the Permitted Third Party become a new party to this DPA in order to use the Services in which case all references to "**Customer**" and "**controller**" in this DPA shall be construed to include the Permitted Third Party.

3. **Definitions and interpretation –** References in this DPA to "**controller**", "**data subject**", "**processor**", "**processing**" (and its derivatives) and "**supervisory authority**" shall have the meaning ascribed to them under the General Data Protection Regulation 2016/679 ("**GDPR**"). References to an "**Annex**" is to an Annex to this DPA. References to "**including**" shall means "including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word". In addition, the terms set out below have the following definitions:

   (a) **AV1** means the AV1 solution and components including the AV1 hardware device and the AV1 apps for mobile and web.

   (b) **Customer** means (i) the entity identified at the start of this DPA in section (A) and/or (ii) a Permitted Third Party that is using the Services pursuant to clause 2.

   (c) **Customer User** means a member of Customer's staff (e.g. teachers for AV1, or residential care home personnel for Komp) who has an AV1 or Komp user account and is authorised to use the Services, or any other person delegated to use the Services by the Customer.

   (d) **End User** means (as applicable) (i) the individual who is the end user of the AV1 (e.g. a student), (ii) the individual who is the end user of the Komp (e.g. the individual who has the Komp in their residence) or (iii) the individual who uses the Komp family mobile app to send messages or video to the Komp.

   (e) **Komp** means the Komp solution and components including the Komp hardware device, the Komp family mobile app and the Komp Pro web app.

   (f) **Permitted Third Parties** means a third party entity (e.g. a school or care home) which Customer permits to use the Services in accordance with clause 2.

   (g) **Personal Data** means any information relating to an identified or identifiable natural person ("**data subject**") (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person) which is processed by Supplier (acting as a processor) on behalf of Customer (acting as a controller), in connection with the provision of Services as described in Annex 1.

   (h) **Privacy Laws** means any data protection and/or privacy related laws, statutes, directives or regulations (and any amendments or successors thereto) to which a party to this DPA is subject and which are applicable to the Services, including the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the United Kingdom Data Protection Act 2018 ("**UK DPA**") and the United Kingdom GDPR (as defined in section 3 of the UK DPA), and any other relevant national privacy legislation.

   (i) **Services** means (as applicable) the provision of the AV1 or Komp solutions and components, support services and any other services described in the relevant Agreement.

   (j) **Subprocessor** means a third party engaged by Supplier (including an affiliate and/or subcontractor of Supplier) in connection with the processing of the Personal Data.

4. **Description of processing and status of the parties**

   (a) A description of the subject-matter and duration of the processing of the Personal Data, the nature and purpose of the processing, and the type of personal data and categories of data subject are set out in Annex 1 to this DPA.

   (b) Unless otherwise expressly stated: (i) this DPA applies solely where Supplier processes Personal Data as a processor on behalf and under the instruction of Customer in connection with the provision of Services and (ii) Customer shall be the controller of the Personal Data and Supplier shall be the processor in respect of the processing of Personal Data in connection with the Services.

5. **Customer obligations** – Customer (as controller) is responsible for complying with applicable Privacy Laws in respect of the processing of the Personal Data, including:

   (a) ensuring there is a valid legal basis in accordance with Privacy Laws for the processing of the Personal Data at

the time it is transferred to Supplier or processed by Supplier in connection with the Services;

(b) ensuring any consent it obtains complies with Privacy Laws and is, in particular, informed, specific, unambiguous and freely given; and

(c) ensuring that any information that must be provided to data subjects about the processing has been given at the proper time.

At the request of Supplier, Customer shall explain in writing and/or document the legal basis for the processing and provide any other information to demonstrate its compliance with this clause.

6. **Instructions for processing**

(a) Subject to clause 6.1(c) below, Customer instructs Supplier to process the Personal Data (i) to provide the Services and give effect to the Agreement and this DPA and (ii) for any of the other purposes set out in Annex 1. Customer may issue additional instructions from time to time **provided that** any such additional instructions must be agreed between the parties in writing.

(b) Instructions may only be issued by Customer's management team, its data protection officer (if any) and/or its head of legal (if any). Those authorised to issue instructions may (at any time, in writing) delegate their authority to others.

(c) Customer is responsible for ensuring its instructions comply with applicable Privacy Laws. However, if Supplier is of the opinion that an instruction is in breach of applicable Privacy Laws, Supplier shall inform Customer promptly and Supplier shall be entitled to suspend the execution of the instruction until such time as the parties agree otherwise in writing.

(d) Supplier is not authorised to process the Personal Data for any purposes other than those specified in Annex 1 or as otherwise agreed between the parties in writing from time to time.

7. **Data deletion and retention**

(a) Subject to clauses 7(b) and 18, upon termination of the Services (for any reason) and if requested to do so in writing by Customer, Supplier shall delete the Personal Data in its possession within sixty (60) days from the date of Customer's request. Deletion means that the Personal Data is permanently deleted from all Supplier systems, except from its backup system (which may only be accessed by Supplier's technical personnel).

(b) Supplier is not required to delete any Personal Data that Supplier must retain in order to comply with applicable law. Such retained Personal Data shall be deleted without undue delay upon expiry of the relevant legal requirement.

(c) If requested by the Customer, Supplier shall confirm in writing that the Personal Data has been deleted.

(d) Supplier shall not make or retain copies of the Personal Data except as permitted under this DPA or with the prior written consent of Customer.

(e) If Customer instructs Supplier (in writing) to delete the Personal Data before completion of the Services (for any reason), the following shall apply:

(i) Supplier shall comply with such instruction within sixty (60) days;

(ii) Supplier shall not be required to provide the Services following deletion of the Personal Data and shall not be liable for any non-compliance with its obligation to provide the Services under the Agreement or this DPA;

(iii) Customer shall pay Supplier for all unpaid fees for Services that Supplier has performed up to date when the Personal Data is deleted.

8. **Security measures –** Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the processing and any other relevant circumstances relating to the processing of the Personal Data, Supplier shall implement (and ensure compliance with) appropriate technical and organisational measures as required by applicable Privacy Laws to ensure a level of security appropriate to any risk associated with the processing of the Personal Data. In particular and where appropriate, Supplier shall:

(a) organise its internal organisation in such a way that the requirements of data protection are complied with (including the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services); and

(b) implement data minimisation measures (such as pseudonymisation and encryption) to limit the amount of stored personal data.

The parties agree that the measures set out in Annex 2 to this DPA provide the required level of security for the protection of Personal Data that meets the requirements of this clause.

9. **Confidentiality** – Supplier shall ensure that the persons it authorises to process the Personal Data (including its employees and Subprocessors) ("**Authorised Persons**") are subject to appropriate obligations of confidentiality. Supplier shall take all reasonable measures to:

(a) ensure the reliability and trustworthiness of Authorised Persons;

(b) ensure Authorised Persons comply with applicable Privacy Laws in respect of their processing of Personal Data;

(c) ensure Authorised Persons are appropriately informed about their obligations under applicable Privacy Laws in respect of the processing of Personal Data; and

(d) monitor the compliance of Authorised Persons with the obligations in this clause.

10. **Personal Data Breach**

(a) Supplier shall notify Customer without undue delay and in any event within seventy-two (72) hours of Supplier becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed as part of the Services ("**Personal Data Breach**"). Such notification shall include at least:

(i) a description of the nature of the Personal Data Breach, including (if possible) the categories and approximate number of data subjects concerned and the Personal Data affected;

(ii) the name and contact details of the data protection officer or other contact where more information can be obtained;

(iii) a description of the likely consequences of the Personal Data Breach; and

(iv) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including (where appropriate) any measures to mitigate its possible adverse effects.

(b) If it is not possible to provide the information in clause 10(a) at the same time, the information may be provided in phases without undue further delay.

(c) If required by applicable Privacy Laws, Customer shall notify the Personal Data Breach to the relevant supervisory authority.

(d) If Customer intends to notify a Personal Data Breach to a supervisory authority, other regulator or law enforcement agency, Customer shall (unless prohibited by law) allow Supplier an opportunity of at least six (6) hours to review the notification. Customer shall have due regard to any reasonable comments or amendments proposed by Supplier.

(e) Insofar as Customer has to comply with obligations to notify affected data subjects in connection with a Personal Data Breach, Supplier shall reasonably cooperate with Customer and provide Customer with any assistance reasonably required.

11. **Subprocessors**

(a) Subject to clause 11(c) below, Supplier is permitted to engage and use Subprocessors to process Personal Data and to disclose Personal Data to Subprocessors in connection with the Services. A list of Supplier's current Subprocessors is available upon request.

(b) Supplier shall notify Customer (which can be done by email, or by posting a notification on the relevant customer facing app or other interface, if any) if Supplier intends to engage a new Subprocessor, or if there are any changes with regard to existing Subprocessors. If Customer has any objections to the proposed new Subprocessor, or to any changes to existing Subprocessors, it must notify Supplier without undue delay and in any event within thirty (30) days from the date of Supplier's notification. Customer may only object on reasonable grounds (including reasonable and documented reasons relating to a Subprocessor's non-compliance with applicable Privacy Laws). If no objection is received by Supplier after expiry of the thirty day period, the additions or changes notified to Customer shall be deemed agreed by Customer. If Customer opposes the notified additions or changes and the parties cannot reach a reasonable solution promptly, Supplier may terminate the Agreement (which shall have the effect of terminating this DPA) with immediate effect in which case Customer shall pay Supplier for all unpaid fees for Services that Supplier has performed up to the date of termination.

(c) Supplier shall ensure it has in place binding agreements in writing with all Subprocessors it engages to process Personal Data for specific processing activities on behalf of Customer and that such agreements impose obligations that are, in substance, the same data protection obligations imposed on Supplier under this DPA.

12. **International data transfers –** The parties do not transfer Personal Data from (i) the European Economic Area ("**EEA**") or the United Kingdom ("**UK**") to (ii) a country that is not subject to an adequacy decision (pursuant to Article 45 of the GDPR or similar provision in UK Privacy Laws) and to which a transfer of Personal Data may only take place subject to compliance with conditions laid down by applicable Privacy Laws ("**Third Country**"). If a transfer is necessary in connection with the provision of Services, such transfer shall only be permitted if:

(a) Customer has given written prior consent to the transfer;

(b) where the transfer is from the EEA to a Third Country, the parties enter into the Standard Contractual Clauses (Module Two: controller to processor) issued by the European Commission on 4 June 2021 (2021/914) ("**SCCs**");

(b) where the transfer is from the UK to a Third Country, the parties enter into the SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for UK transfers of Personal Data dated 21 March 2022 (or any subsequent version).

13. **Record of processing and privacy impact assessments** – Supplier shall provide reasonable cooperation and assistance to Customer in connection with any data protection impact assessment(s) which applicable Privacy Laws require Customer to carry out in relation to the processing of the Personal Data in connection with the Services, including any required prior consultation(s) with supervisory authorities. Supplier reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

14. **Data subject rights** – Supplier shall, at Customer's expense and to the extent required in connection with the Services, provide the necessary assistance to enable Customer to respond to requests from data subjects exercising their rights under applicable Privacy Laws (including the right of access, correction and deletion) in respect of any Personal Data. Supplier shall (to the extent applicable given the nature of the processing and the Personal Data that is processed by Supplier) promptly and in any event within ten (10) working days correct or delete the Personal Data on the instructions of Customer. If Supplier receives a request from a data subject exercising their rights under applicable Privacy Laws, Supplier shall forward that request to Customer without undue delay.

15. **Audit rights**

(a) Subject to clause 15(b), Supplier shall upon reasonable prior written request of at least thirty (30) days (unless a shorter notice period is required by applicable Privacy Laws, an order of a supervisory authority or in the event of a Personal Data Breach) make available to Customer all information necessary to demonstrate compliance with the obligations set out in this DPA and applicable Privacy Laws and allow for and contribute to audits, including inspections, conducted by Customer or an external auditor appointed by the Customer.

(b) Customer's right under clause 15(a) does not apply to the extent it would disclose any personal data, information or confidential information received by Supplier from other customers.

(c) Any audit shall be carried out during normal business hours and without affecting the regular business operations of Supplier and in compliance with Supplier's onsite policies and procedures.

(d) Customer has the right to carry out an audit only once a year (unless required more frequently by applicable Privacy Laws, an order of a supervisory authority, or in the event of a Personal Data Breach).

(e) If Customer appoints an external auditor to carry out the audit, the auditor shall be bound by a duty of confidentiality. Supplier reserves the right to require any such third party to execute a confidentiality agreement directly with Supplier prior to the commencement of an audit.

(f) Except where the audit discloses a failure on the part of Supplier to comply with its material obligations under this DPA, Customer shall pay all reasonable costs and expenses (including any charges for the time engaged by Supplier, its personnel and professional advisers) incurred by Supplier in complying with this clause 15. However, if the audit reveals a failure on the part of Supplier to comply with its material obligations under this DPA, Supplier shall pay all reasonable costs and expenses (including the reasonable costs of any external auditor) incurred by Customer.

(g) Customer shall provide to Supplier a copy of any audit reports generated in connection with an audit carried out under this clause 15 unless prohibited by applicable law. The audit report shall be considered confidential information of the parties.

16. **Liability** – Without prejudice to any liability which either party may have under applicable Privacy Laws, each party's liability under this DPA shall be limited to the amounts and types of liability set out in the Agreement.

17. **Termination and suspension**

(a) This DPA remains in effect until such time as the Agreement is terminated for any reason.

(b) In the event of a breach of this DPA by Supplier, Customer may require Supplier to suspend processing of any or all of the Personal Data with immediate effect until such time as the breach is resolved or, if it is not capable of being resolved, the DPA is terminated for breach in accordance with the terms of the Agreement.

18. **Supplier use of derived data**

(a) Customer agrees to Supplier using metadata and other analytics data including usage data and statistical analysis data (each of the foregoing in anonymised format) which Supplier obtains as a result of providing the Services ("**Derived Data**") for the purpose of research and development, including developing, enhancing and/or improving Supplier's services and the products and solutions offered and provided to its customers.

(b) Supplier shall not disclose any Derived Data that is traceable to Customer to any third parties (other than to Supplier's Subprocessors) unless permitted under this DPA, or the disclosure is required in order to comply with applicable law.

(c) Supplier shall not be required by Customer to return or delete Derived Data upon termination of the Services (for any reason). If Customer is compelled by a legally binding order (e.g. of a court or regulatory authority of competent jurisdiction) to have the Derived Data deleted, then Supplier agrees, as legally required, to delete the Derived Data that is the subject of the binding order as soon as practicable following receipt of a certified copy of such binding order.

19. **Notices and variations**

(a) All notices related to this DPA shall be sent in writing to the e-mail address specified in Annex 1 (Contact section).

(b) If there is a change to applicable Privacy Laws, or if a judgment or statement from a competent authority or other authoritative source changes the interpretation of any applicable Privacy Laws, or if changes are made to the delivery of Services under the Agreement that require a change to be made to this DPA, the parties shall cooperate in good faith to update the DPA without undue delay. Any change or addition to this DPA shall be made in writing and signed by both parties.

20. **Applicable Law** – The choice of law and venue that shall apply to this DPA shall be the same as for the Agreement.

21. **Execution** – This DPA may be executed in any number of counterparts, each of which shall, when executed and delivered, be deemed an original and all counterparts taken together shall constitute one and the same instrument. An executed counterpart of the entire DPA (not just the signature page) may be delivered by e-mail (as a scanned pdf or other agreed format).

By signing below, each part enters into this DPA:

Signed for and on behalf of Customer by its duly authorised representative:	
Signature:	
Name (print):	
Position:	
Place/date:	

Signed for and on behalf of Supplier by its duly authorised representative:	
Signature:	
Name (print):	
Position:	
Place/date:	

Annex 1
Description of processing and Subprocessors

Purpose for processing

For BOTH AV1 and Komp: Personal Data is processed in connection with the provision of the relevant Services for the purpose of:

- administering and managing the relevant Services, including onboarding customers
- providing Customer with statistical and other information on use of the Services
- creating and managing Customer accounts and authenticating Customer Users
- tracking when AV1 and Komp are enabled; tracking use of AV1 and Komp once enabled
- providing technical support services to both Customer Users and End Users (including investigating support issues and troubleshooting)
- implementing security measures and issue resolution.

For AV1: further processing purposes include:

- enabling the deployment and use of AV1s for the purpose of streaming live video
- managing AV1 inventory (e.g. generating keywords for new users; creating an overview of all AV1s).

For Komp: further processing purposes include:

- offering communication services to End Users, including displaying images and messages on screen, and streaming video
- creating a log of Komp Pro communications (including metadata) to enable Customer to maintain a record of activities carried out on the Komp.

Categories of data subjects

For AV1: Categories of data subjects whose Personal Data may be processed are: AV1 End Users and Customer Users. Other individuals with whom the AV1 interacts that may be identifiable via the AV1 live stream video (e.g. students and teachers).

For Komp: Categories of data subjects whose Personal Data may be processed are: Komp End Users including Komp mobile app users (these are individuals connected to the Komp via the family app who may send messages, video and other content to the Komp End Users) and Customer Users. Other individuals that may be included in pictures, livestream video or in text messages sent to the Komp who may be identifiable.

Types of Personal Data processed

For BOTH AV1 and Komp:

- Customer User contact details (e.g. name, telephone number, email address)
- Customer User account information (e.g. name, email, unique user ID) which is visible to other Customer Users within the Customer organisation
- For support services, End User contact details (e.g. name and telephone) may be processed if End User requests such services. In this situation it is possible, for example, for a student and/or family member to request support services and provide their name and/or username
- IP addresses may be processed to establish connections between End User, Customer Users and AV1 and/or Komp
- Serial number for AV1 or Komp
- Metadata created from use of AV1 or Komp, including network information (WiFi/4G) and usage data, such as when the device was last used.

For AV1: Individuals may be seen on the live video stream, but live video stream is not otherwise stored, cached, or processed.

For Komp: Types of Personal Data processed are:

- name and profile picture of individuals calling the Komp (so that End User can identify the caller)
- other personal identifiers such as room number of a nursing home or initials of the End User
- pictures and messages sent to the Komp that can identify individuals
- name and telephone number for individual signing up for a family member account
- video streams
- user logs containing information about: time and duration of video calls, who made the call, when a picture was sent, when a message was sent, sender identity (name and ID) and End User identity (serial number and name)
- activity logs and entire logs for Komp use. The activity logs are given in the interface for PRO users with access to the same Komp and only contain the name of the sender.

Processing activities

For AV1 and Komp: Personal Data will be subject to the following processing activities in respect of both the AV1 and Komp: collection (e.g. collection of metadata when AV1 and Komp are in use), creation (e.g. accounts and user logs), organisation, data input, structuring, storage, backup, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available (including through video streaming), erasure or destruction.

Duration of processing

For AV1 and Komp: Supplier deletes Personal Data in accordance with its internal retention and disposal policy, and the provisions of clause 6 of this DPA. Data relating to the connection between Customer and AV1 or Komp will be deleted when the AV1 or Komp is returned to Supplier after use.

For Komp: Customer can select the retention period for messages, pictures and other content sent to the Komp. Such content will be deleted from the Komp after the set expiration date/time. Content that is not deleted by Customer will be stored during the term of the Agreement. Upon termination of the Agreement, all such content will be deleted (including from back up systems) in accordance with clause 6 of this DPA.

Subprocessors

For AV1 and Komp: Supplier uses Subprocessors in the provision of the Services. A list of current Subprocessors is available upon request.

Contact details

Customer contact details: As set out in the order confirmation documentation.

Supplier contact details: privacy@noisolation.com

Annex 2
Technical and organisational security measures

Security measures for No Isolation products and services

In this Annex 2 the following definitions are used:

- "**Premises**" means the office premises from which Supplier operates, including in Norway, Germany and the UK; and
- "**Systems**" means collectively (i) any computers, servers, networks and data processing systems and (ii) applications and software (including SaaS) – whether on-premise or in the cloud – which are used by Supplier to provide the Services.

Technical security measures and business continuity

Access rights and restrictions

- Measures are in place to prevent unauthorised persons from using or accessing Systems and ensure such authorised persons can only access data in accordance with their allocated access authorisation.
- Only authorised persons have access to Systems in which Personal Data and metadata are stored. Access to Systems is granted on a need-to-know basis and is monitored and logged.
- Supplier's internal and customer-owned management systems use role-based access controls, restricting the ability to modify or delete data to specific customer organisations and authorised user groups.
- Access to Systems and cloud-based accounts is based on an allocated user ID and two-factor-authentication.
- Systems are only exposed to a minimal set of endpoints that must be exposed in order for Services to be provided. The exposed endpoints only support HTTPS and all clients (e.g. Komp or AV1) must be authenticated by the System before the endpoints can be used. Measures are in place to check who has entered, changed or removed Personal Data in the Systems.
- Access for remote diagnosis is only granted upon approval from Customer. Remote diagnosis sessions are logged and, depending on access level required, support personnel must present a physical hardware authentication key to start the remote diagnosis session.
- Additional logical separation is enforced within Supplier's software through the use of fixed and unique customer and device identifiers and secure temporary session-based tokens generated on successfully authenticated connections.
- Access to Supplier's infrastructure is subject to security rules and regulations that only allow traffic from authorised sources. Access to resources on the infrastructure is limited to Supplier administrators (operations personnel) who need access to perform maintenance on the Systems.

Data integrity

The following measures are in place to ensure stored Personal Data cannot be corrupted by system malfunctions:

- database and data storage systems are maintained through continuous application of maintenance measures, recommendations and vendor best practices; and
- all procedures by which Personal Data is entered, stored and manipulated are designed with integrity and security safeguards built in. All such procedures are thoroughly tested and peer reviewed prior to implementation.

Encryption

- All transmission of data over the internet related to AV1 or Komp is encrypted to at least the TLS 1.2 standard and covers transmissions required for the Services.
- All signals are encrypted with strong keys and use HTTPS protocol.
- Databases/servers have encrypted disks/backups/ communications.
- All media traffic (i.e. audio and video stream) use SRTP (with DTLS for key exchange) or DTLS. Communications are encrypted end-to-end with these keys using SRTP whether communications take place directly between the AV1 or Komp to the apps, or through a relay).
- Metadata (including IP address, end point identifiers and encryption keys) required to establish connections is sent encrypted with TLS between AV1 or Komp and Supplier's servers. The WebRTC standard is used to set up the audio and video stream and WebRTC signals (i.e. metadata) are transmitted (TLS-encrypted) via Supplier servers.

Intrusion detection and incident handling

- Networked Systems are secured against unauthorised intrusion through firewalls, endpoint protection services, monitoring and management tools.
- Supplier's infrastructure is designed to log information about system behaviour, traffic received, system authentication and other application requests. Internal systems will alert relevant personnel of any malicious, unintended or atypical activities. Supplier's personnel, including security, operations and support personnel are trained to respond to identified security incidents.
- Records are maintained of identified security incidents. Suspicious and confirmed security incidents are investigated and appropriate resolution steps are documented. For confirmed security incidents, a post-security incident review is conducted by Supplier and appropriate actions are taken to minimise the risk of damage or unauthorised disclosure.

Monitoring

- Supplier continuously monitors its Systems with direct notifications to operational personnel if any Systems fail.
- Monitoring applications are deployed and configured to monitor System capacity and alert operations personnel when predefined thresholds are reached.
- **Komp:** Supplier uses services such as AWS Shield and Amazon GuardDuty and follows industry practices when developing and running its Systems.

Passwords, keywords and PINs

- Supplier's password policy requires a minimum length (8 characters) and a strong password (no repeating or consecutive characters).
- **AV1:** To access an AV1 for the first time, the End User must have a unique keyword associated with that AV1. After entering the keyword in the app, the End User must create a PIN code which must be re-entered each time the app is opened.
- **Komp**: To access a Komp for the first time, the End User must have a unique keyword associated with that Komp. After entering the keyword in the app, the End User must provide their mobile phone number to create an account. Upon subsequent logins a one-time code will be delivered via SMS that must be used. Additional End Users can be invited to the associated Komp by generating additional one-time codes within the Komp app.
- **For AV1 and Komp web apps** (i.e. AV1 Admin and Komp Pro): Customer Users must log in with email and password.

Screen locks

For Supplier personnel, a password-protected automatic screen lock is enforced, with training and policies encouraging personnel to manually lock their screens when leaving their desk.

Virus protection, hacking and DOS

- Anti-virus software is installed on all computers and is centrally monitored and managed.
- Supplier protects its Systems from hacking (e.g. AWS Shield is a managed Distributed Denial of Service protection service which protects applications running on AWS).

Business continuity and disaster recovery

- Supplier maintains a business continuity plan ("**BC Plan**") which has procedures to protect against disruptions caused by unexpected events and includes reporting channels, emergency contacts, formation of response teams and contingency plans for critical systems. The BC Plan is tested annually, with results and improvements managed as part of Supplier's Information Security Management System.
- Supplier uses cloud services to ensure data and services are available when needed. Supplier backs up critical systems every 24 hours. Backups are stored in the cloud to enable systems to be restored quickly, if necessary, at a different location (e.g. in the event of damage such as fire or power failures).

- Software and configuration information relating to the Systems and internally developed and managed application services are managed in a secured source code repository. Supplier can quickly restore or redeploy application services if needed. This includes the option of relocating the services to another location if required.
- Business continuity, disaster recovery and incident response routines are deployed by Supplier's cloud infrastructure provider and SaaS providers (who use commercially reasonable efforts to ensure uptime, redundant power, network and HVAC services).

Network and transmission security measures

Cloud

Only authorised Supplier personnel have access to the Systems including the AWS console and login is secured by unique username, secure password and two-factor authentication.

Network

- The System is only available through a minimal number of endpoints to provide services to Customer and Users. Endpoints only support HTTPS. Customer Users/End Users must authenticate themselves within the System before endpoints can be used. Authentication serves as access control if an AV1 or Komp is under attack. It is not possible for a potential attacker to gain access to additional AV1s or Komps, even if the attacker has access to a specific AV1 or Komp.
- Access to operating equipment is only available via SSH and SSH keys are password protected.

Signal transmission

AV1 and Komp communicate through two channels.

- **AV1**: First channel is used for signal transmission with signals passing through Supplier's servers. This is used for metadata such as the battery level and the availability of the AV1 on the internet. This metadata is made available to Customer User and End User, as well as to Supplier's customer service team for support services. The second channel creates a direct media channel between the AV1 and the app to enable End User to connect to and use the AV1. Media traffic is routed over the shortest network route between the AV1 and the app, with high bandwidth and low latency being critical for audio and video streaming.
- **Komp**: First channel is used for signal transmission with signals passing through Supplier's servers. This is used for transferring content (e.g. messages/images sent to the Komp) and metadata (including availability of the Komp on the internet). Metadata is available to Customer User/End User (via their app) and Supplier's customer service team for support services. The second channel creates a direct media channel between the Komp and the app to enable audio and video call stream. Media traffic is routed over the shortest network route between the Komp and the app, with high bandwidth and low latency being critical for audio/video streaming.

Physical security measures

Alarm/CCTV – All Premises are equipped with burglar alarm systems and video surveillance at the entrances and exits, managed and maintained by the landlords.

Access rights and restrictions

- Measures are in place to prevent unauthorised persons from gaining access to the locations where Systems are held.
- Supplier personnel are trained in procedures for securely locking and unlocking Premises.

Keys

- Supplier personnel must use individual PIN protected key cards or traditional physical keys (depending on location) to access Premises.
- Keyed personnel are included in the equipment list held by the office manager in Norway and delegated to directors in Germany and UK.
- Visitors must be accompanied by Supplier personnel at all times.

Network access

In Germany and the UK, Supplier's landlords are responsible for implementing controls to secure physical access to the networks they provide, which Supplier uses to conduct its local operations.

Organisational security measures

Certifications

- Certifications held by Supplier include UK Cyber Essentials and ISO 27001, both of which have been independently validated.
- Services are hosted by a cloud infrastructure provider that maintains independently validated certifications (including ISO 27001 and SOC 2) that are reviewed annually.

Compliance checking and auditing

Supplier has measures to document essential processing to enable its data processing systems to be checked for compliance with Supplier's obligations (including compliance with Customer's instructions).

Confidentiality

Supplier's has contracts with its personnel (including employees, consultants and contract workers) that include confidentiality obligations. The duty of confidentiality continues after the employment has ended and for as long as the information remains confidential.

Controlled documentation

Supplier maintains a set of controlled documentation to support its secure operations and to maintain its Information Security Management System (ISMS). Controlled documents are reviewed quarterly and approved by management.

Employee controls

- Supplier ensures its employees are aware of their responsibilities with regard to the processing of Personal Data through Supplier's "Acceptable Use Policy" and its "Code of Conduct".
- The effectiveness of these controls is regularly verified through internal audits conducted by Supplier's compliance officer, who forwards any observations to the relevant IS/security officer for follow-up within the Information Security Management System (ISMS). Typically, these audits take the form of interviewing a random sample of employees to confirm compliance with established policies and procedures.

Policies and procedures

- Supplier's "Access Control Policy" sets out the responsibilities of system owners and administrators, including the rules and procedures for adjusting permissions and the need for continuous review of access to all systems operated by Supplier.
- Supplier personnel must comply with Supplier's "Remote Working Policy" which outlines safe remote working practices for the physical environment in which work is carried out.
- Supplier personnel must comply with Supplier's "Acceptable Use Policy" which defines the appropriate handling of data (e.g. clear desk and clear screen policy).

Third parties

- Amazon Web Services EMEA SARL and the SaaS software suppliers are responsible for implementing controls to manage physical access to operational and server premises.
- Access to third-party servers is governed by Supplier's data processing agreements with server providers.

Review and assessment

- Supplier continuously conducts risk-based monitoring of controls and control testing follows a formal methodology. Test results are documented and reviewed by senior management, including any plans to correct any deficiencies found.
- Supplier performs security risk assessments on third-party providers whose services store, process or transmit data from Supplier and/or Customers. Supplier conducts a bi-annual operational security risk assessment of production applications, services and broader business processes, documented in a risk register.

Training

- Managers are responsible for ensuring Supplier personnel are appropriately trained (given their areas of responsibility).
- Supplier personnel have received information about social hacking (e.g. phishing, social engineering, fraud) and how it can be avoided.