Data Processing Agreement

(“Agreement)

(based on the annex to the European Commission implementing decision on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3701, June 4th, 2021)

between

The Customer

(natural or legal person that has entered into a main service agreement with No Isolation)

(hereafter referred to as the “Controller”)

and

No Isolation

(No Isolation AS, No Isolation Ltd, or No Isolation GmbH, as applicable)

(hereafter referred to as the “Processor”)

Each a “Party” and jointly the “Parties”

SECTION I

Clause 1

Parties and Applicable No Isolation Entity

(a) This Agreement is entered into between the Controller and the No Isolation company entity that is the contracting party under the applicable main service agreement for the provision of the AV1 solution (the "Main Service Agreement"), which consists of No Isolation's Terms and Conditions together with any applicable order documents accepted by the Controller. All references to the "Processor" in this Agreement shall be understood to refer to the relevant No Isolation entity identified as the contracting party under the applicable Main Services Agreement.

(b) Depending on the entity named in the Main Service Agreement, the contracting party for this Agreement shall be:

- No Isolation AS, Pilestredet 28, 0166 Oslo, Norway
- No Isolation Ltd, 201 Borough High Street, London, England, SE11JA
- No Isolation GmbH, Innere Wiener Straße 11, 81667 München, Germany

Clause 2

Purpose and scope

(a) The purpose of this Agreement is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) These Clauses apply to the processing of personal data as specified in Annex I.

(c) Annexes I to III are an integral part of the Clauses.

(d) These Clauses are without prejudice to obligations to which the Controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(e) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 3

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 4

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the written agreement of all Parties, accede to them at any time as a Controller or a Processor by completing the relevant Annexes and providing written notice of accession to the other Parties.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, as applicable.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 7

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex I.

Clause 8

Obligations of the Parties

8.1. Instructions

(a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

8.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Controller.

8.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Annex I.

8.4. Security of processing

(a) The Processor shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

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

8.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the Processor shall apply specific restrictions and/or additional safeguards.

8.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

(c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

8.7. Use of sub-processors

(a) The Processor has the Controller's general authorisation for the engagement of sub-processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

(b) Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data Processor in accordance with these Clauses. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The Processor shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations.

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

8.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The Controller agrees that where the Processor engages a sub-processor in accordance with Clause 8.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

c) To increase the stability and security of their infrastructure, the Processor might use services of a company (and respectively its parent company) that is located in the USA. This may result in the transfer of personal data to the USA. This transfer is based on the adequacy decision of the European Commission (Art. 45 (1) GDPR) as the service provider is registered under the EU-US Data Privacy Framework (DPF). Even in the event that changes are made to this decision or the decision will be revoked, the transfer is secured and legitimated by contractual, technical and organisational measures according to Art. 44 et seqq. GDPR, as described in clause 8.8 b).

Clause 9

Assistance to the Controller

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

(b) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

(c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex II the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 10

Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the Processor.

10.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

10.2 Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

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

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex II all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller’s obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 11

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the Processor has been suspended by the Controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the Processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 8.1 (b), the Controller insists on compliance with the instructions.

(d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

ANNEX I: DESCRIPTION OF THE PROCESSING

The AV1 solution is designed to support the inclusion of people who are unable to attend school for extended periods. The solution consists of the AV1 telepresence robot ("AV1") and the AV1 app installed on the end user's device. The Controller can also manage its AV1s and view statistical usage data in the web-based portal AV1 Admin. As all references made to an AV1 unit are by a pseudonym and the Processor has no reasonable means for re-identification, no usage data can be linked to an identifiable individual by the Processor.

The AV1 enables real-time livestreaming of audio and video data from the classroom to the end user's device (such as a mobile phone or tablet). Audio is transmitted from the student's app to the AV1. The AV1 allows the student to remotely follow classroom activities from home while enabling classmates and teachers to see and respond to the student's signals and participation. All transmission occurs live, and no audio or video recordings are stored.

Details on the type and scope of the processing of personal data is based on the contractual obligations specified in the Main Service Agreement between the parties.

In principle, the processing of special categories of personal data within the meaning of Article 9 Regulation (EU) 2016/679 (herinafter referred to as "GDPR") is not part of the main contractual agreements.

Insofar as special categories of data are processed in individual cases (e.g. in the context of making available video and audio content), appropriate technical and organisational measures shall ensure that, in particular, the requirements of the principles of data minimisation and compliance with the principle of confidentiality are adequately taken into account.

The duration of the processing (clause 8.3) is based on the duration of the respective Main Service Agreement between the parties.

The nature of the processing is as follows: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination and erasure of data.

Service Module 1: "Delivery of AV1 and AV1 Admin" (Infrastructure)

The purpose of the processing under this service module is to deliver the agreed services, in particular to:

- administer and manage the relevant services, including onboarding customers,
- create and manage customer accounts and authenticating customer users
- manage AV1 inventory (e.g. generating keywords for new users; creating an AV1 asset list)
- provide customer with statistics on the usage of the AV1
- track when AV1 is enabled; tracking use of AV1 App once enabled
- implement security measures and issue resolutions

Categories of personal data processed in this module are:

- Contact data (title, name, e-mail, workplace, function, etc.)
- Access data (e-mail address, credentials)
- IT traffic and usage data (IP address (non-persistent), date and time of access etc.)
- Other information that may be entered by the data Controller in the free-text fields of the AV1 Admin portal.

- Robot allocation ID
- Usage statistics*
- Reasons for AV1 allocation*

*Usage statistics and allocation reasons are processed on behalf of the Controller as part of the AV1 solution, as stated in the Main Service Agreement. They are also aggregated to analyze usage and improve the Processor's services. More information can be found in No Isolation's privacy policy.

Categories of data subjects are:

- "Customer user" (member of staff in the educational organization authorized to use the service)
- "End user" (person using the AV1 app)

Declaratory note:
In addition, unless the function has been deactivated on the explicit instructions of the controller, the following pseudonymized data—anonymized from the perspective of the processor—may also be processed:

- Reason for using AV1 (specified in categorized form):

  Somatic Illness or Injury, mental health conditions (SEMH), early intervention to prevent school non-attendance, special educational needs (SEN), behavioral support and temporary exclusion, displacement, transitional or unstable living situations, disability, high ability remote learners, alternative educational programs, other reasons)

- Gender of the user

  This data is provided to the processor by the controller via the technical infrastructure in a form that is anonymized for the processor and is used to provide the controller with statistical evaluations on the use of the AV1 avatars. It is impossible for the processor to draw conclusions about natural persons and thus establish a link to individuals. In this respect, no order processing takes place for this data.

The controller is solely responsible for verifying the lawfulness of the processing for anonymization (before the aforementioned data is transmitted).

Categories of data subjects in this module:
Personal data are collected from the "customer user" (i.e., member of the staff of the educational organization, who is authorized to use the service) and "end user" (i.e., students using the AV1 app or their parents).

Service Module 2: "AV1 and the AV1 App" (Livestream)

The purpose of the processing under this service module is to enable delivery and use of livestreaming between a mobile device (e.g., iPad) and AV1, specifically to provide the end user with the technical means to participate in education and other school activities from a different location.

Categories of personal data processed in this module are:

- (Encrypted) audio and video data (non-persistent)
- Metadata (length and quality of the video transmission, date and time, wireless network information, signal strength, mobile network information).
  IP addresses (non-persistent).

Categories of data subjects are:

- Customer user
- End user
- *Other students, teachers or customer employees in the classroom or other physical persons in connection with a school activity

*Audio and video data is transmitted as part of the livestream to the end user. This data is never stored and is therefore non-persistent. The livestream is end-to-end encrypted, and no one except the end user can access it, including the data Processor.

Service Module 3: "Technical Support"

The purpose of the processing under this service module is to provide technical support services to both customer users and end users (including investigation of support inquiries and troubleshooting).

Types of personal data processed in this module include:

- Contact details (e.g., name, email address, phone number).
- Content data in written communication between the data Controller and the data Processor, which in individual cases may contain personal data.
- Metadata (length and quality of the video transmission, date and time, wireless network information, signal strength, mobile network information).

Categories of data subjects are:

- Customer users
- End users
- Employees of both the Controller and the Processor
- "Customer user" (member of staff in the educational organization authorized to use the service)

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

Compliance with data processing security requirements pursuant to Art. 32 GDPR Measures to protect confidentiality, integrity, and availability	
Pseudonymisation, anonymisation, and encryption of personal data	☒ Pseudonymisation End user receives a pseudonymized user ID through the Controller. The Processor does not get knowledge of the user's identity. ☒ Encryption ☒ Data in transit ☒ Data at rest Encryption is realized with TLS 1.2 and AES256-bit. ☒ Anonymisation All metadata is anonymized when there is no longer an active subscription for the AV1.
Confidentiality of processing systems and services	☒ Physical access control (physical control) All premises are equipped with burglar alarm systems and video surveillance at the entrances and exits, managed and maintained by the landlords. Measures are in place to prevent unauthorised persons from gaining access to the locations where systems are held. No Isolation personnel are trained in procedures for securely locking and unlocking premises. No Isolation 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 No Isolation personnel at all time. ☒ System and data access control (organisational / technical control) 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.

	No Isolation'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. Access to No Isolation'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 No Isolation administrators (operations personnel) who need access to perform maintenance on the Systems.
Integrity of processing systems and services	Event logging (e.g., during authentication or CRUD actions - create, read, update, delete data): ☒ *Input control (Verification at what time and by whom personal data was entered, modified or deleted)* Systems are exposed only to a minimal set of endpoints necessary to provide services. The exposed endpoints only support HTTPS, and all clients must authenticate against 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. Database and data storage systems are maintained through continuous application of maintenance measures, recommendations, and vendor best practices; 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. ☒ Transmission and forwarding control *(Verification to which entities personal data have been transmitted)* All transmission of data over the internet related to AV1 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 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 and No Isolation'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 No Isolation servers.
Availability of processing systems and services and ability to restore availability and data access after a physical or technical incident	☒ Recoverability (Recovery / Backup) No Isolation 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). No Isolation 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 No Isolation's Information Security Management System Software and configuration information relating to the Systems and internally developed and managed application services are managed in a secured source code repository. No Isolation can quickly restore or redeploy application services if needed. This includes the option of relocating the services to another location if required. ☒ Reliability control (reporting of malfunctions, failures, and threats) Networked Systems are secured against unauthorised intrusion through firewalls, endpoint protection services, monitoring and management tools. No Isolation's infrastructure logs 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. No Isolation'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 and appropriate actions are taken to minimise the risk of damage or unauthorised disclosure. 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. ☒ Availability (redundancies of systems and infrastructure) Business continuity, disaster recovery and incident response routines are deployed by No Isolation's cloud infrastructure provider and SaaS providers (who use commercially reasonable efforts to ensure uptime, redundant power, network and HVAC services). ISO 27001 policies e.g., for vulnerability management, backup, risk management, patch management, reveal a managed approach to information security goals. Infrastructure is provided by AWS with separated environments for design/test (staging) and production. Availability is constantly monitored.
Processing personal data only on documented instructions from the Controller, and separately for the respective purposes	☒ Order control *(personal data are processed only in accordance with the instructions of the client)* No Isolation 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. 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. Pursuant to this Agreement, No Isolation is obliged to process data only on documented instructions. Staff is being informed and trained accordingly. It is specified which people may give and receive instructions for processing. ☒ Data separation *(personal data collected for different purposes are processed separately*).

	Additional logical separation is enforced within No Isolation's software using fixed and unique customer and device identifiers and secure temporary session-based tokens generated on successfully authenticated connections.
Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	☒ Information Security Officer (ISO) appointed ☒ Information Security Management System (ISMS)
Evidence of data processing security in the form of certifications or recognized organizational measures.	*Relevant certifications* ☒ ISO 27001 – Information Security Management System The information on controls is credibly verifiable via documented concepts and guidelines within the scope of ISO 27001 certification

ANNEX II – LIST OF SUBPROCESSORS

The Controller has authorized the use of the following subProcessors pursuant to Clause 8.7(a):

1. Amazon Web Services EMEA SARL
   38, Avenue John F. Kennedy
   1855 Luxembourg
   Luxembourg

   Subject of the assignment:
   Cloud infrastructure services

   Processing in: EU
   Data centre location: Frankfurt am Main, Germany

   The subProcessor has contractually obliged themselves to solely host the data in Frankfurt. Transfers are not expected to occur, unless strictly necessary for support purposes or compliance with national US laws.

   As appropriate safeguards within the meaning of Articles 44 et seq. GDPR, a data processing agreement was concluded using the Standard Contractual Clauses (SCCs) of the European Commission (as of June 2021). As supplementary measures, data protection-friendly configuration settings were selected (data minimization) and appropriate technical measures such as pseudonymization were implemented.

2. No Isolation AS*
   Pilestredet 28
   0166 Oslo
   Norway

   Subject of the assignment:
   Provision of customer services (CRM)

   Processing in: EEA (Norway)

3. No Isolation Ltd*
   201 Borough High Street
   London
   SE11JA
   United Kingdom

   Subject of the assignment:
   Provision of customer services (CRM)

Processing in: UK

Third country processing under adequacy decision of the Commission according to Art. 45 GDPR.

4. No Isolation GmbH*
   Innere Wiener Straße 11
   81667 Munich
   Germany

   Subject of the assignment:
   Provision of customer services (CRM)

   Processing in: EU (Germany)

*The use of No Isolation entities as sub-Processors depends on which No Isolation entity is party to the agreement.