IRIS Connect: Organisation Administrator & Data Processing Agreement 1.4

Version	Date	Change
1.0	March 2010	Document Creation
1.1	Feb 2017	General Improvements
1.2	April 2018	GDPR Compliance
1.3	November 2020	Restructured the document to make it easier to read and broken the contents down into sections to make navigation easier. Used guidance from The European Data Protection Board to revise our agreement so that it more closely follows their guidance. Added 2 additional sub-processors (see section 4, appendix B for our approved sub-processors). Updated the document to reflect the new ways of recording using IRIS Connect, including video conferencing with IRIS Connect Rooms, Screen Capture and Call Recording.
1.4	April 2024	Added Microsoft Azure & OpenAI as Sub-Processors Addition of Appendix D - SCCs to cover OpenAI use by EU-based customers Addition of Appendix E - International Data Transfer Addendum to the EU Commission Standard Contractual Clauses to cover OpenAI use by UK-based customers *Full list of changes can be found here*

Table of Contents

1. Preamble

1.1 This is an agreement between the entity you represent ("Customer", "you" or "your") that for the purposes of this agreement will be acting as the Data Controller, and for customers located in:

i) the EEA or Switzerland, IRIS Connect/iConnect (Ireland) Limited;
ii) the US, IRIS Connect Inc.;
iii) the UK, Oceania or anywhere else other than the EEA, Switzerland, or the US, IRIS Connect Limited and/or trading as iConnect ("IRIS Connect");

will provide the Services and contract with Customer and for the purposes of this agreement will be acting as Data Processor.

1.2 These Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

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

1.4 In the context of the provision of the IRIS system, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

1.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

1.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor.

1.9 Appendix D contains Standard Contractual Clauses. This is only for EEA-based customers using either the: 1) AI Insights feature with OpenAI 2) Call Recording feature

1.10 Appendix E contains the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses. This is only for UK/Oceania-based customers using either: 1) AI Insights feature with OpenAI 2) Call Recording feature

1.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other relevant legislation.

2. Definitions

2.1. Capitalised terms
Capitalised terms used but not defined in this Agreement have the meanings given elsewhere in the applicable Agreement. In this Agreement, unless stated otherwise:

"**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

"**Additional Security Controls**" means security resources, features, functionality and/or controls that a Customer may use at its option and/or as it determines. "Additional Security Controls" may include the Admin Console and other features and functionality of the Services such as two factor authentication, security key enforcement and monitoring capabilities.

"**Advertising**" means online advertisements displayed by IRIS Connect to End Users, excluding any advertisements the Customer expressly chooses to have IRIS Connect or any of its Affiliates display in connection with the Services under a separate agreement.

"**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the applicable Agreement, either per annual period or event giving rise to liability, as applicable.

"**Agreement Effective Date**" means the date on which the Customer clicked to accept or the parties otherwise agreed to this Agreement in respect of the applicable Agreement

"**Audited Services**" means the Services listed as audited in the IRIS Connect Service Summary.

“Applicable data protection law” see “Local Regulatory Framework”

“Approved Partner” means those approved by IRIS Connect to represent them in specific regions. A full list can be found in the IRIS Connect website Privacy Policy

“Basic/Content Licence” is a feature restricted account on the IRIS Connect Web Platform. Users are able to consume content but not upload.

“Closed Account” means when an Organisation’s access to their IRIS Connect Accounts is terminated.

“**Complementary Product Agreement**” means: any other agreement under which IRIS Connect agrees to provide identity services as such to the Customer; or any other agreement that incorporates this Agreement by reference or states that it will apply if accepted by the Customer.

“**Complementary Product Services Summary**” means the then-current description of the services provided under a Complementary Product Agreement, as set out in the applicable Agreement.

“**Community Group**” means a group on the IRIS Connect platform which enables sharing and collaboration between two or more organisations

“**Customer Data**” means data submitted, stored, sent or received via the Services by the Customer, its Affiliates or End Users.

“**Customer Personal Data**” means personal data contained within the Customer Data.

“**Data Incident**” means a breach of IRIS Connect’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by IRIS Connect. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“**EEA**” means the European Economic Area.

“European Union and UK Data Protection Legislation” means, as applicable: (a) the GDPR; and/or (b) the GDPR as defined in section 3(10) (as supplemented by section 205(4)) of the DPA 2018 (UK GDPR) GDPR.

“**Full Activation Date**” means: (a) if this Agreement is incorporated into the applicable Agreement by reference, the Agreement Effective Date; or (b) if the parties otherwise agreed to this Agreement, the eighth day after the Agreement Effective Date.

“Full Licence” means full access to the IRIS Connect Web Platform’s features.

“**GDPR**” means 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, and repealing Directive 95/46/EC.

“Hardware (Camera)” includes any products purchased from IRIS Connect, including the Discovery Kit and Starter Kit

“**IPRs**” Intellectual property rights

“**IRIS Connect System**” means the Core Services for IRIS Connect, as described in the IRIS Connect Services Summary.

“**IRIS Connect’s Third Party Auditor**” means an IRIS Connect-appointed, qualified and independent third party auditor, whose then-current identity IRIS Connect will disclose to the Customer.

“**IRIS Connect Services Summary**” means the then-current description of the Core Services for IRIS Connect, (as may be updated by IRIS Connect from time to time in accordance with the Agreement).

“Local Regulatory Framework” means the legislation, law or regulation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the state/territory in which the data controller is established;

“**Non-European Union Data Protection Legislation**” means data protection or privacy legislation other than the European Union and UK Data Protection Legislation.

“**Notification Email Address**” means the email address(es) designated by the Customer in the Admin Console or the Order Form to receive certain notifications from IRIS Connect.

“Organisation Administrator”: Data Protection Officer or Senior Person within the Customer organisation who is responsible for overseeing the management of IRIS Connect within the organisation.

“Rules of Conduct” are defined within the End User Licence Agreement (EULA) Section 3.1.

“SCCs” are the EU standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

"**Security Documentation**" means all documents and information made available by IRIS Connect under Clause 10 and on our Support Hub.

"**Security Measures**" means the security measures set out in Appendix C

"**Services**" means the following services, as described in the IRIS Connect Service Summary

"**SOC 2 Report**" means a confidential Service Organisation Control (SOC) 2 Report (or a comparable report) on IRIS Connect's systems examining logical security controls, physical security controls, and system availability, as produced by IRIS Connect's Third Party Auditor in relation to the Audited Services.

"**Subprocessors**" means third parties authorised under this Agreement to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.

"**Term**" means the period from the Agreement Effective Date until the end of IRIS Connect's provision of the Services under the Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which IRIS Connect may continue providing the Services for transitional purposes.

"**Third Party Providers**" means organisations who you may choose to engage with via the IRIS Connect platform.

"User" is anyone who has an IRIS Connect account, is considered to be a 'User

"User Content" is any User created content uploaded to the IRIS Connect Web Platform including video, audio, images, attachments, comments and Groups.

"UK Addendum" is the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses. See Appendix E

2.2. Clarification of Terms

The terms "personal data","special categories of data", "data subject", "process/processing", "controller", "processor" and "supervisory authority" as used in this Agreement have the meanings given in the GDPR in each case irrespective of whether the European Union and UK Data Protection Legislation or Non-European Union Data Protection Legislation applies.

SECTION 1: ORGANISATION ADMINISTRATOR AGREEMENT

3. Data Management

3.1 The monitoring, recording, holding and processing of images of distinguishable individuals constitutes personal data as defined by the General Data Protection Regulation ("GDPR"). This Agreement is intended to ensure that in the use of IRIS Connect it is compliant with the requirements of GDPR, with related legislation and with the CCTV Code of Practice published by the Office of the Information Commissioner.

3.2 While the IRIS Connect system does contain a feature to apply anonymisation filters, you acknowledge that recorded data may still represent personal data (for example if it is triangulated with other sources to identify an individual). Users must use their own judgement to decide if the anonymisation filters have sufficiently obfuscated data subjects before sharing any data.

3.3 If your intended use of the system is likely to collect personal data, you agree to do so in a way which is compliant with the requirements of the GDPR or applicable local regulatory framework. This may include but is not limited to the following:

3.3.1 Documenting your legal basis for processing personal data

3.3.2 Ensuring appropriate transparency and privacy notices

3.3.3 Ensuring robust mechanisms for ensuring ongoing compliance

3.3.4 Providing appropriate channels for appeal

3.3.5 Ensuring appropriate registration with the Information Commissioner's Office (ICO)

3.3.6 Adopting a balanced and reasonable policy to managing Subject Access Requests (SARs) and third party disclosures which safeguards the rights of all data subjects and respects the original purpose of the data collection

3.3.7 Enforcing data retention periods in line with your Organisation's Data retention policy

Further support around legal processing is available on the IRIS Connect website.

3.4 A nominated Organisation Administrator (who must be authorised by your organisation to make decisions about the management of their data) must manage the Organisation's compliance with this

Agreement. By using the Organisation Administrator Account, the Organisation Administrator agrees the following on behalf of the organisation:

3.5 Management of Content

Your organisation is the data controller for all data uploaded by Users at your organisation to the IRIS Connect system. Your designated Organisation Administrator/s is responsible for making day to day decisions about the management of recorded data, permissioning collaboration groups, data sharing and the monitoring of data recorded by your Organisation.

3.5.1 IRIS Connect provides a content oversight tool which enables Organisation Administrators to review randomised thumbnail images from videos recorded within the organisation. This tool is designed to enable the identification of inappropriate content. You agree to only use this tool for this sole purpose.

3.5.2 You will be responsible for the management and monitoring of data owned by your Organisation. If a User at your organisation flags an issue with a recording or any other content, you agree that you are responsible for investigating the issue and for ensuring that any inappropriate content is removed.

4. System Management

4.1 A nominated Organisation Administrator (who must be authorised by your Organisation to make decisions about the management of their data) must manage the Organisation's compliance with this Agreement. By using the Organisation Administrator Account, the Organisation Administrator agrees the following on behalf of the organisation:

4.2 Management of Users

Unless Users in your organisation are enrolled on a third party provider programme you will be responsible for the creation/amendment/deletion/suspension & management of the User accounts at your Organisation. If a leaving User chooses to transfer any data that they are managing to the Organisation Administrator – you will be bound by the EULA as if that data was your own.

4.2.1 If you use your Organisation Administrator Account to create additional Organisation Administrator Accounts then you confirm that;

4.2.1.1 you understand that the User for that account will be required to comply with these same terms;

4.2.1.2 that any additional Organisation Administrator Accounts will only be created for individuals that you warrant are entitled to and in a position to sign up to such terms;

4.2.1.3 you are responsible for the actions of any User using an Organisation Administrator Account that you have issued them, any breach of the Organisation EULA by that User will be deemed as a breach of the Organisation EULA by yourself;

4.2.1.4 you will only create User accounts for employees, students or trainees at your organisation.

4.3 Management of Scope:

You are required to monitor User requests for engagement with third party providers and other organisations on the IRIS Connect platform to provide, deny or revoke permission for Users from your organisation to share data and participate in collaborative activities.

4.3.1 third party providers may have additional terms as part of their service subscription. You acknowledge that while you will always retain overall rights to uploaded data, these agreements may include additional conditions. For example third party agreements may introduce new stipulations for the management and ownership of non-video IPRs generated by course participants.

4.3.2 You acknowledge that agreeing to such conditions represents a contract between you and the third party provider and agree to be bound by their terms and monitor User engagement to ensure organisational compliance.

4.3.3 On the IRIS Connect system Organisation Administrators may authorise the creation of groups which enable Users to share recorded data and collaborate with Users from other organisations. Such “community groups” enable Organisation Administrators to create participation agreements to be agreed by all members of the group.

4.3.4 You agree that if you authorise your Users to participate in community groups you agree to be bound by the terms you have agreed to and to monitor User engagement to ensure compliance

4.3.5 You acknowledge that if you or another admin has approved inter-organisational sharing via a group (via approving access to or upgrading to a community group) that.... you are responsible for ensuring that inter-organisation sharing is appropriate and proportional and that the participation agreement clearly identifies the following :

4.3.5.1 What data may be shared and in what format

4.3.5.2 The purpose for the data sharing and for how long it will be shared

4.3.5.3 Such additional provisions as are necessary to ensure legal processing both within your organisation and collaborating organisations

4.3.6 You agree to ensure that group administrators that are users of your organization meet their obligations in terms of content moderation and appropriate access to the groups they manage.

4.4 Management of Use:

The IRIS Connect system is for professional development, educational research and learning development, consequently, you agree:

4.4.1 To ensure that the use of the system is aligned with the stated purpose and that the system is not used for surveillance of staff or learners

4.4.2 To ensure that use of the system complies with the End User Licence Agreement (EULA) including, but not limited to:

4.4.2.1 To use the system to promote better learning outcomes

4.4.2.2 That all Users conduct themselves in a professional manner, to not use the system to bully or intimidate other Users or data subjects

4.4.2.3 To ensure recorded content is appropriate to and aligned with the purpose

4.4.2.4 To make sure recording equipment is positioned so it's visible, safely located and unlikely to record data which is not required or not for the purpose you are using the system

4.4.2.5 To make sure Users are empowered to report to the Organisation Administrator, content or use that does not meet the above criteria

4.4.2.6 To ensure Users maintain system security and don't share passwords

4.5 Management of Privacy and Disclosures:

The IRIS Connect system incorporates a privacy by design philosophy which on a day-to-day basis gives Users control of the following:

4.5.1 When reflections are made and deleted

4.5.2 Who has access to reflections and how long for

4.5.3 Your participation in live reflections

4.5.4 The creation of groups and the content thereof

4.6 In exceptional circumstances IRIS Connect will enable managed onsite review or third party disclosures in situations where the following are being investigated either by the organization, or law enforcement agency:

4.6.2.1 Suspected system misuse and severe breaches of the EULA

4.6.2.2 Suspected professional misconduct

4.6.2.3 Suspected criminality

4.7 GDPR requires that personal data collected for one purpose cannot be further processed for another, incompatible purpose. If the sound and images recorded for professional development are subsequently used in an investigation, you agree that you will ensure you have a lawful basis to use the sound and images for this new purpose.

4.8 The IRIS Connect Web Platform (https://app.irisconnect.com) is a secure service for the selective sharing of recordings. Role based log in and encrypted communications ensure that the recordings are secure and managed within the privacy by design model. Under normal operation, recordings and other data may not be downloaded from the web platform.

4.9 If we receive a formal request from the data controller we will enable resources to be downloaded from the platform. You agree that in these circumstances IRIS Connect will cease to be the data processor of the resources downloaded from the platform and the organisation will be fully responsible for the data and responsible for any damages caused by a breach or security or privacy.

SECTION 2: DATA PROCESSING AGREEMENT

5. Data Processing

5.1 Commencement and Duration of Data Processing Agreement

This Agreement will take effect on the Agreement Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion or return of all Customer Data by IRIS Connect as described in this Agreement.

5.2 Separate Agreement

If a separate DPA has been signed, that agreement takes precedence over any similar provisions contained in other agreements between the parties, including this Agreement.

5.3 Future Rulings

The Data Processor and Data Controller will monitor all future rulings that may affect these agreements and commit to working together in good faith to alter them or make any additional provisions required of any clear ruling, within this specified time frame given within the ruling

5.4 Application of European Legislation

The parties acknowledge and agree that the European Union and UK Data Protection Legislation will apply to the processing of Customer Personal Data if, for example:

5.4.1 The processing is carried out in the context of the activities of an establishment of the Customer in the territory of the UK and/or EEA; and/or

5.4.2 The Customer Personal Data is personal data relating to data subjects who are in the UK and/or EEA and the processing relates to the offering to them of goods or services in the UK and/or EEA or the monitoring of their behaviour in the UK and/or EEA.

5.5 Non European Union Data Controllers

For data controllers located outside of the European Union and the UK, IRIS Connect commits to process your data in accordance with your Local Regulatory Framework.

5.6 Processor and Controller Responsibilities

If the European Union and UK Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

5.6.1 The subject matter and details of the processing are described in Appendix A

5.6.2 IRIS Connect is a processor of that Customer Personal Data under the European Union and UK Data Protection Legislation;

5.6.3 The Customer is a controller or processor, as applicable, of that Customer Personal Data under the European Union and UK Data Protection Legislation; and

5.6.4 Each party will comply with the obligations applicable to it under the European Union Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.7 Authorisation by Third Party Controller

If the Customer is a processor, the Customer warrants to IRIS Connect that the Customer's instructions and actions, with respect to that Customer Personal Data, including its appointment of IRIS Connect as a sub-processor, have been authorised by the relevant controller of that data.

5.8 Additional Products

If IRIS Connect at its option makes any Additional Products available to the Customer in accordance with the Additional Product Terms (if applicable), and if the Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Agreement does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by the Customer, including personal data transmitted to or from such Additional Products. The Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services.

5.9 IRIS Connect's Processing Records

The Customer acknowledges that IRIS Connect is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which IRIS Connect is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, the Customer will, where requested, provide such information to IRIS Connect via the Admin Console or other means provided by IRIS Connect, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

5.10 IRIS Connect's Data Protection Team

IRIS Connect's Data Protection Team can be contacted via the Support Desk.

5.11 The Parties' Agreement on Other Terms

The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR or Local Regulatory Framework..

6. The Rights and Obligations of the Data Controller

6.1 The data controller is responsible for ensuring

6.1.1 that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the state/territory where the data controller is established) and does not violate the relevant provisions of that state/territory. For clarity for our EU customers this means the GDPR (see Article 24 GDPR), the applicable EU or member state data protection provisions, and the Clauses.

6.1.2 that it has instructed and throughout the duration of the personal data-processing services will instruct the data processor to process the personal data transferred only on the data controller's behalf and in accordance with the applicable data protection law and the Clauses;

6.1.3 that the data processor has provided sufficient guarantees in respect of the Security Measures specified in Appendix C to this contract;

6.1.4 that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

6.1.5 that it will ensure compliance with the security measures required for the applicable data protection law;

6.1.6 to make available to a data subject upon request a copy of the Agreement, with the exception of Appendix C, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Agreement, unless the Agreement or the contract contain commercial information, in which case it may remove such commercial information;

6.1.7 that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 17 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data processor under the Agreement;

6.1.8 that it will ensure compliance with Clause 6.1.

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

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

6.4 Monitoring implementation of this Agreement rests with nominated Organisation Administrators/Data Protection Officer (DPO) and IRIS Connect.

6.5 For the purpose of the GDPR, Organisation Administrators are nominated as Data Protection Officer (if no DPO has been required to be nominated under GDPR).

7. The Obligations of the Data Processor

7.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by UK, Union or Member State law to which the processor is subject. In such a case, the data processor shall inform the data controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Agreement.

7.2 The data processor shall immediately inform the data controller:

7.2.1 if instructions given by the data controller, in the opinion of the data processor, contravene the Local Regulatory Framework or GDPR or the applicable EU or state data protection provisions;

7.2.2 If it cannot provide such compliance with its instructions or the Agreement for whatever reasons;

7.2.3 of any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

7.2.4 of any accidental or unauthorised access including a Data Incident; and

7.2.5 of any request received directly from a data subject without responding to that request, unless it has been otherwise authorised to do so;

7.3 The data processor is responsible for ensuring

7.3.1 that it has implemented the Security Measures specified in Appendix C before processing the personal data transferred and maintains the Security Measures for the duration of the processing;

7.3.2 to deal promptly and properly with all inquiries from the data controller relating to its processing and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

7.3.3 at the request of the data controller to submit its data-processing facilities for audit of the processing activities covered by the Clause, which shall be carried out by the data controller or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data controller , where applicable, in agreement with the supervisory authority, as outlined in Clause 13

7.3.4 to make available to a data subject upon request a copy of the Agreement, or any existing contract for sub-processing, unless the Agreement or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix C which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data controller;

7.3.5 that, in the event of sub-processing, it has previously informed the data controller and obtained its prior written consent as outlined in Clause 17.

7.3.6 that the processing services by the sub-processor will be carried out in accordance with Clause 17;

7.3.7 that upon request will send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data controller.

7.4 Customer's Instructions

By entering into this Data Processing Agreement, the Customer instructs IRIS Connect to process Customer Personal Data only in accordance with applicable law:

7.4.1 to provide the Services and related technical support;

7.4.2 as further specified via the Customer's use of the Services (including the Admin Console and other functionality of the Services) and related technical support;

7.4.3 as further documented in any other written instructions given by the Customer and acknowledged by IRIS Connect as constituting instructions for purposes of this Data Processing Agreement.

7.5 IRIS Connect's Compliance with Instructions

As from the Full Activation Date, IRIS Connect will comply with the instructions described in Section 7.3 (Customer's Instructions) (including with regard to data transfers) unless Local Regulatory Framework or EU law to which IRIS Connect is subject requires other processing of Customer Personal Data by IRIS Connect, in which case IRIS Connect will inform the Customer (unless that law prohibits IRIS Connect from doing so on important grounds of public interest) via the Notification Email Address.

7.5.1 IRIS Connect will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services.

7.5.2 IRIS Connect does not allow any third parties to view or modify customer data outside of the purpose of providing the contracted services.

7.6 Impact Assessments and Consultations

IRIS Connect will (taking into account the nature of the processing and the information available to IRIS Connect) assist the Customer in ensuring compliance with any obligations of the Customer in respect of data protection impact assessments and prior consultation, including if applicable, the Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

7.6.1 providing the Additional Security Controls in accordance with Section 10 (Security of Data Processing) and the Security Documentation

7.6.2 providing the information contained in the applicable Agreement

8. Confidentiality

8.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On

the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

8.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

9. Erasure and Return Of Data

9.1 Deletion During Term

IRIS Connect will enable the Customer and/or End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If the Customer or an End User uses the Services to delete any Customer Data during the applicable Term, this use will constitute an instruction to IRIS Connect to delete the relevant Customer Data from IRIS Connect's systems in accordance with applicable law. Delete requests are processed automatically following instructions via the Data Controller. Data is held in a trashed state for 90 days then a further 180 days in data back-ups

9.2 Deletion on Term Expiry

Subject to Section 9.3 (Deferred Deletion Instruction), on expiry of the applicable Term, the Customer may instruct IRIS Connect to delete all Customer Data (including existing copies) from IRIS Connect's systems in accordance with applicable law. Delete requests are processed automatically following instructions via the Data Controller. Data is held in a trashed state for 90 days then a further 180 days in data back-ups. Without prejudice to Section 14.1 (Access; Rectification; Restricted Processing; Portability), the Customer acknowledges and agrees that the Customer will be responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain afterwards.

Upon termination of a paid license agreement the Data Controller will decide whether to;
a) renew the licence, or
b) download and/or delete their data, or
c) continue on a free Basic Licence.

If no Customer Users access their data for 2 years (no logins by any user within a 2 year period) the Data Processor will delete the data. Prior to deletion, the Data Processor will send at least 2 email notifications to the Data Controller. The Data Controller will instruct the Data Processor if they want to download their data prior to deletion, or renew their licence. No reply from the Data Controller to the deletion notification email will result in the deletion of the data.

9.3 Deferred Deletion Instruction

To the extent any Customer Data covered by the deletion instruction described in Section 9.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 9.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such

Customer Data when the continuing Term expires. For clarity, this Data Processing Agreement will continue to apply to such Customer Data until its deletion by IRIS Connect.

9.4 Return of Data

As outlined in Section 19, upon expiry of the applicable Term the Customer may instruct the IRIS Connect to return the video data transferred to the Customer.

9.5 IRIS Connect will process the requests as outlined in Section 9.1 - 9.4 unless legislation imposed upon it prevents it from returning or destroying all or part of the personal data transferred. In that case, the IRIS Connect warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

10. Security of Data Processing

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

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

a. Pseudonymisation and encryption of personal data;

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

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

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

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

10.4 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data

processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

10.5 If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, if applicable the data controller shall specify these additional measures to be implemented in Appendix C.

10.6 IRIS Connect's Security Measures, Controls and Assistance

IRIS Connect will implement and maintain technical and organisational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in the Security Controls and Measures document. The Security Controls and Measures document includes measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of IRIS Connect's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. IRIS Connect may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

10.7 Security Compliance by IRIS Connect Staff

IRIS Connect will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data are aware of their and IRIS Connect's obligations under the European Union and UK Data Protection Legislation, and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10.8 Additional Security Controls

In addition to the Security Measures, IRIS Connect will make the Additional Security Controls available to:

10.8.1 Allow the Customer to take further steps to secure Customer Data; and

10.8.2 Provide the Customer with information about securing, accessing and using Customer Data.

10.8.3 Additional Security Controls are outlined in the Security Measures and Controls Document

10.9 IRIS Connect's Security Assistance

IRIS Connect will (taking into account the nature of the processing of Customer Personal Data and the information available to IRIS Connect) assist the Customer in ensuring compliance with any of the Customer's obligations in respect of security of personal data and personal data breaches, including if applicable the Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

10.9.1 Implementing and maintaining the Security Measures in accordance with Section 10.6 (IRIS Connect's Security Measures);

10.9.2 Making the Additional Security Controls available to the Customer in accordance with Section 10.8 (Additional Security Controls);

10.9.3 Complying with the terms of Section 11 (Data Incidents); and

10.9.4 Providing the Customer with the Security Documentation in accordance with Section 13 (Audi and Inspection) and the information contained in the applicable Agreement.

11. Notification of Data Incidents or Personal Data Breach

11.1 Incident Notification

If IRIS Connect becomes aware of a Data Incident, IRIS Connect will: (a) notify the Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data. Further information about IRIS Connect's Data Breach Response and Notification Procedure can be found here.

11.2 Details of Data Incident

Notifications made pursuant to this section will describe, to the extent possible:

a) details of the Data Incident including the nature of the Data Incident, and the categories and approximate number of both data subjects and personal data records concerned;

b) steps taken to mitigate the potential risks and steps IRIS Connect recommends the Customer take to address the Data Incident and

c) the likely consequences of the Data Incident.

11.3 Delivery of Notification

Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address. IRIS Connect may in addition to an email, deliver a notification of any Data Incident(s),by direct communication (for example, by phone call or an in-person meeting). The Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

11.4 No Assessment of Customer Data by IRIS Connect

IRIS Connect will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. The Customer is solely responsible for complying with incident notification laws applicable to the Customer and fulfilling any third party notification obligations related to any Data Incident(s).

11.5 No Acknowledgment of Fault by IRIS Connect

IRIS Connect's notification of or response to a Data Incident under this Section 8.2 (Data Incidents) will not be construed as an acknowledgement by IRIS Connect of any fault or liability with respect to the Data Incident.

11.6 Assisting the Data Controller

11.6.1 IRIS Connect will reasonably co-operate with the Customer in the Customer's handling of the matter, including:

(a) assisting with any investigation;

(b) making available all relevant records, logs, files, data reporting and other materials required to comply with European Union and UK Data Protection Legislation or as otherwise reasonably required by the Customer; and

(c) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Data Incident or unlawful Personal Data processing.

12. Customer's Security Responsibilities and Assessment

12.1 Customer's Security Responsibilities

The Customer agrees that, without prejudice to IRIS Connect's obligations under Section 10.6 (IRIS Connect's Security Measures, Controls and Assistance) and Section 11 (Data Incidents):

12.1.1 The Customer is solely responsible for its use of the Services, including:

12.1.1.1 making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data and

12.1.2.2 securing the account authentication credentials, systems and devices the Customer uses to access the Services

12.1.2 IRIS Connect has no obligation to protect Customer Data that the Customer elects to store or transfer outside of IRIS Connect's and its sub-processors' systems (for example, offline or on-premise storage),

12.1.3 IRIS Connect has no obligation to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent the Customer has opted to use them.

12.4 Customer's Security Assessment

The Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and IRIS Connect's commitments under this Section 10 (Security of Data Processing) will meet Customer's needs, including with respect to any security obligations of the Customer under the European Union and UK Data Protection Legislation and/or Non-European Union Data Protection Legislation, as applicable.

12.5 The Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by IRIS Connect as set out in Section 10.6 (IRIS Connect's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

12.6 Security Certifications and Reports

IRIS Connect will do the following to evaluate and help ensure the continued effectiveness of the Security Measures:

12.6.1 maintain Cyber Essentials Plus (or higher) certification

12.6.2 Review the following sub-processor reports and certifications as they are updated to ensure they maintain or improve on their existing security standards:

a. SOC 2
b. SOC 3
c. ISO 9001
d. ISO 27001
e. ISO 27017
f. ISO 27018

13. Audit and Inspection

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

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

13.3 Internal Security Documentation

In addition to the information contained in the applicable Agreement, IRIS Connect will make available for review by the Customer the following documents and information to demonstrate compliance by IRIS Connect with its obligations under this document:

13.3.1 The IRIS Connect Security Measures and Controls document

13.3.2 DfE Cloud Service Providers certificate and independent audit

13.3.3 Cyber Essentials Plus certificate

13.4 Sub Processor Security Documentation

13.4.1 Amazon
Amazon's security documentation can be found here:
https://aws.amazon.com/compliance/programs/ and here: https://aws.amazon.com/security

13.4.2 **OpenAI**
Open AI's security documentation can be found here:https://openai.com/security/

13.4.3 Microsoft Azure
Microsoft Azure's security documentation can be found here:
https://learn.microsoft.com/en-us/azure/compliance/

13.5 Customer's Audit Rights

IRIS Connect will allow the Customer or an independent auditor appointed by the Customer to conduct audits (including inspections) to verify IRIS Connect's compliance with its obligations under this Data Processing Agreement in accordance with Section 13.7 (Additional Business Terms for Reviews and Audits). IRIS Connect will contribute to such audits as described in Section 12.6 (Security Certifications and Reports) and this Section 13 (Audit and Inspection).

13.6 The Customer may also conduct an audit to verify IRIS Connect's compliance with its obligations under this Data Processing Agreement by reviewing the Security Documentation (which reflects the outcome of audits conducted by IRIS Connect's Third Party Auditor).

13.7 Additional Business Terms for Reviews and Audits

The Customer must send any requests for reviews of the Security Measures and Controls document or audits to IRIS Connect's Data Protection Team via the Support Desk.

13.7.1 Following receipt by IRIS Connect of a request IRIS Connect and the Customer will discuss and agree in advance on:

13.7.2.1 the reasonable date(s) of and security and confidentiality controls applicable to any review of the Security Measures and Controls Document.

13.7.2.2 the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.

13.8 IRIS Connect may charge a fee (based on IRIS Connect's reasonable costs) for any audit provided that IRIS Connect will not charge a fee, or will reimburse the Customer for any fees paid, in connection with an audit where IRIS Connect is found to have breached these Clauses of the Local Regulatory Framework.. IRIS Connect will provide the Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. The Customer will be responsible for any fees charged by any auditor appointed by the Customer to execute any such audit.

13.8 IRIS Connect may object in writing to an auditor appointed by the Customer to conduct any audit if the auditor is, in IRIS Connect's reasonable opinion, not suitably qualified or independent, a competitor of IRIS Connect, or otherwise manifestly unsuitable. Any such objection by IRIS Connect will require the Customer to appoint another auditor or conduct the audit itself.

14. Data Subject Rights

14.1 Access; Rectification; Restricted Processing; Portability

During the applicable Term, IRIS Connect will, in a manner consistent with the functionality of the Services, enable the Customer to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by IRIS Connect as described in Section 9.1 (Deletion During Term), and to export Customer Data.

14.2 Data Subject Requests

14.2.1 Customer's Responsibility for Requests

During the applicable Term, if IRIS Connect receives any request from a data subject in relation to Customer Personal Data, IRIS Connect will advise the data subject to submit his/her request to the Customer, and the Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

14.3.1 IRIS Connect's Data Subject Request Assistance

The Customer agrees that (taking into account the nature of the processing of Customer Personal Data) IRIS Connect will assist the Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

14.3.1.1 providing the Additional Security Controls in accordance with Section 7.3 (Additional Security Controls); and

14.3.2.1 complying with the commitments set out in Section 12.1 (Access; Rectification; Restricted Processing; Portability) and Section 12.2.1 (Customer's Responsibility for Requests).

15. Assistance to the Data Controller

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

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

15.2.1 the right to be informed when collecting personal data from the data subject

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

15.2.3 the right of access by the data subject

15.2.4 the right to rectification

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

15.2.6 the right to restriction of processing

15.2.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

15.2.8 the right to data portability

15.2.9 the right to object

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

15.3 In addition to the data processor's obligation to assist the data controller pursuant to Clause 10.4 (Security of Data Processing)., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

15.3.1 The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent

supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

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

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

15.3.4 the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

15.4 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 15.1. and 15.2.

16. Transfer of Data to Third Countries or International Organisations

16.1 Data Storage and Processing Facilities

IRIS Connect will store and process Customer Data in compliance with the requirements of the data legislation for your country. For EU customers this means that we will store your data within the EU. For a UK customer, we will continue to store your data in the EU, although we commit to transferring your data to the UK should a change in data protection law require it.

16.2 Data Centre Information

IRIS Connect Users Amazon AWS storage to store all of Customer Data. Detailed Information about these data centres is available here.

16.3 Location of Customer Data

16.3.1 Customers using the Europe platform (https://europe.irisconnect.com) data will be stored in Dublin, Ireland using Amazon AWS servers

16.3 .2 Customers using the US platform (https://us.irisconnect.com) data will be stored in North Virginia, America using Amazon AWS servers

16.3 .3 Customers using the Oceania platform (https://oceania.irisconnect.com) data will be stored in Sydney, Australia using Amazon AWS servers

Further information refer to Appendix B

16.4 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller. Such a transfer would always take place in compliance with Chapter V GDPR for our EU customers and in compliance with Local Regulatory Framework for our customers outside of the EU including the UK . IRIS Connect shall ensure that whenever personal data is transferred to a sub-processor outside the EU and UK they:

16.4.1 are Processing Personal Data in a territory which is subject to a current finding by the Information Commissioner's Office or European Commission under the European Union and UK Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals;

16.4.2 participate in a valid cross-border transfer mechanism under the European Union and UK Data Protection Legislation, so that the parties can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR; or

16.4.3 otherwise ensure that the transfer complies with the Data Protection Legislation.

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

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

16.6.1 transfer personal data to a data controller or a data processor in a third country or in an international organisation

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

16.6.3 have the personal data processed in by the data processor in a third country

16.7 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

16.8. IRIS Connect staff may access customer data for the sole purpose of fulfilling our obligations to the data processor. All access to data is carefully performed following secure processes and procedures.

17. Use of Sub-processors

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

17.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior specific written authorisation of the data controller.

17.3 The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation 30 days prior to the engagement of the concerned sub-processor, either by sending an email to the Notification Email Address or via the Admin Console. The list of sub-processors already authorised by the data controller can be found in Appendix B.

17.4 The Customer may object to any new sub-processor by terminating the applicable Agreement immediately upon written notice to IRIS Connect, on condition that the Customer provides such notice within 90 days of being informed of the engagement of the Sub-processor as described in Section 19.8 (Termination of this Agreement by the Customer). This termination right is the Customer's sole and exclusive remedy if the Customer objects to any new Sub-processor.

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

17.6 The data processor shall therefore be responsible for requiring that:

> **17.6.1** the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.
>
> **17.6.2** the sub-processor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it

17.7 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

17.8 The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the

sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

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

SECTION 3: COMMERCIAL TERMS

18. Subscription Fees & Payment Terms

18.1 Free and Chargeable Services

IRIS Connect offers a blend of free and paid for products and services. Free services or licences provided free of charge or paid for by a third party are exempt from the conditions in this section and our payment terms.

18.2 Subscription Fees and Payment Terms

Upon receipt of a purchase order from either an IRIS Connect Partner or directly, IRIS Connect will issue an invoice for the hardware and software licence. Terms of payment are within 30 days of delivery of the hardware.

18.3 Hardware (Camera)

> **16.3.1** If payment is made in full upon start of the contract, ownership of the camera hardware is transferred to the Organisation.
>
> **16.3.2** If payment is made via financing then the camera hardware is owned by the financing company. Payment can be made at the end of the contracting period to own the hardware.

18.4 Licence Term (Initial Purchase)

The Licence Term is defined by the length of service stated in the purchase order for the product ordered that was submitted to either an IRIS Connect Partner or directly to IRIS Connect, starting from the time of delivery of the hardware or creation of the Organisation Administrator Account on the IRIS Connect Platform, whichever, is later.

18.5 Licence Renewal

The Organisation Administrator will be contacted prior to the end of the licence term to discuss renewing the subscription by IRIS Connect or an Approved Partner. If a renewal licence is purchased this Agreement will be extended by the period stated in the renewal licence product.

19. Commencement,Termination and/or Suspension of Account

19.1 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

19.2 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

19.3 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Section 9 (Erasure) the Clauses may be terminated by written notice by either party.

19.4 If an event occurs under Section 19.5, you will be able to access the system for a period of 60 days following the termination to download any recordings the Organisation wishes to retain.

19.5 By IRIS Connect: Termination of the System

IRIS Connect does not guarantee that it will continue to offer access to the System or support the system. Subject to Section 19.8 IRIS Connect may cease to provide any or all of the services offered in connection with IRIS Connect (including access to the System and any or all features or components of the system), terminate the Agreement, close all Accounts and cancel all of the rights granted to you under the Agreement. IRIS Connect may communicate such termination to you upon 30 days notice in any of the following manners:

19.5.1 when you log into your Account;or

19.5.2 via electronic mail; or

19.5.4 in another manner that IRIS Connect deems suitable to inform you of the termination.

19.6 If IRIS Connect terminates the Agreement pursuant to this section, IRIS Connect will promptly reimburse the subscription on a pro-rata basis and the cost of hardware less 33% depreciation per annum.

19.7 By IRIS Connect for Breach or Misconduct: Suspension of Account

Without limiting IRIS Connect's rights or remedies, IRIS Connect may inform the Organisation of its intention to discontinue or suspend access to the System through the Organisation’s Account in the event of:

19.7.1 a breach of this Agreement by the Organisation or any User under the Account; or

19.7.2 unauthorized access to the System or use of the system by the Organisation or any User under the Account. IRIS Connect has no obligation to reimburse the Organisation on a pro rata basis for a suspended account. The Organisation will have 30 days to satisfactorily remedy the breach or the Agreement will be terminated in accordance with Section 19.8.

19.8 Termination of this Agreement

IRIS Connect may terminate this Agreement, close your Account, and cancel all rights granted to you under the Agreement if:

19.8.1 your Organisation fails to pay the subscription fee when due;

19.8.2 IRIS Connect is unable to verify or authenticate any information you provide that is material to the performance of the Agreement;

19.8.3 you or anyone using any of your Account materially breaches this Agreement, makes any unauthorised use of the System or Software, or infringes the rights of IRIS Connect or any third party;

19.8.4 IRIS Connect becomes aware of uses under your Account that are deemed, at IRIS Connect's discretion, inappropriate or in violation of the Rules of Conduct as set out in the End User Licence Agreement, Section 3.1. Such termination shall be effective upon notice transmitted via electronic mail, or any other means reasonably calculated to reach you.

19.8.4.1 Such termination shall be effective upon notice transmitted via electronic mail (read receipt to be provided evidence), or any other means reasonably calculated to reach the Organisation which may be evidenced by a signed for delivery receipt. The Organisation will have 30 days to satisfactorily remedy the breach prior to termination.

19.8.4.2 IRIS Connect reserves the right to terminate any Accounts that share the name, phone number, e-mail address or internet protocol address with the Closed Account. Termination by IRIS Connect under this section shall be without prejudice to or waiver of any and all of IRIS Connect's other rights or remedies, all of which are expressly reserved, survive termination, and are cumulative. You will not receive a refund of prepaid subscription fees for a termination pursuant to this section.

19.9 Termination of this Agreement by the Customer

You may terminate this Agreement with regard to your Account at any time, upon notice to IRIS Connect via electronic mail. Subject to the exceptions below you will not receive a refund of prepaid subscription fees in the event of such termination.

19.9.1 A Change in this Agreement

If an amendment alters a material commercial term of this Agreement (not amendments required by changes to applicable law) that is unacceptable to you, you may, as your sole and exclusive remedy, terminate this Agreement and close your Account by: clicking the "Sign Out" button when you are prompted to review and agree to the amended Agreement and notifying IRIS Connect via electronic mail within thirty (30) days after the amended Agreement was communicated to you, provided that you have not clicked the "Accept" button or accessed the System during that period.

Your notice must state: that you do not agree to the amended Agreement, specifically describing the amendment(s) with which you disagree, and request IRIS Connect to close your Account. If you click "Accept" or otherwise continue to access the System, you shall be deemed to have accepted the amended Agreement and waive your rights to terminate under this section. IRIS Connect will reimburse the subscription fees on a pro-rata basis and the cost of hardware less 33% depreciation per annum.

19.9.2 System Unavailable 30 Days

The Organisation may terminate this Agreement if the IRIS Connect Platform is not available for 30 days continuously. IRIS Connect will reimburse the subscription fees on a pro-rata basis and the cost of hardware less 33% depreciation per annum.

19.9.3 Termination due to IRIS Connect Breach

The Organisation may terminate this Agreement, and close the Account if IRIS Connect Ltd materially breaches this Agreement, breaches the GDPR or any relevant legislation or infringes the rights of any third party.

a) Such termination shall be effective upon notice transmitted via electronic mail (read receipt to be provided as evidence), or any other means reasonably calculated to reach IRIS Connect Ltd which may be evidenced by a signed for delivery receipt.

19.9.4 Termination due to Non-Renewal of Subscription/Licence

If the Organisation does not renew the subscription agreement then the following procedure occurs IRIS Connect will communicate to you via email to advise & seek a response to the following options:

19.9.4.1 Confirm all data and Users be deleted

19.9.4.2 Request all or some recordings be provided for download.

19.9.4.3 Option to downgrade to a free Basic/Content User licence account

If no response is received:

19.9.4.4 Your Organisation and Users will be downgraded to a Basic/Content User account (this will have reduced functionality as specified by IRIS Connect at its discretion).

19.9.4.5 Data will be held for 12 months from the last activity on the Basic/Content Account.

19.9.4.6 If no activity is recorded on the Platform during that 12 month period. Then the data & Users accounts will be deemed a Closed Account (see section 19.4) without further notice.

19.10 Closed Accounts

If for any reason this Agreement is terminated with regard to your Account, that Account will be closed, upon which all rights granted to you under this Agreement shall terminate with regard to the Closed Account, and you must discontinue your use of the Software, and you may not access the System or any Closed Account, and all the attributes of the Accounts.

19.11 Account Access

Customers whose Accounts have been closed may not access the System in any manner or for any reason, including through any other Account, without the express written permission of IRIS Connect. Users of active accounts may not knowingly allow former Users whose Accounts have been closed to use the active User's Account..

19.12 Deletion of Data

All Customer Data will be deleted from our systems as per section 9.2. (Deletion on Term Expiry)

20. Licences

20.1 Software License

Subject to the terms of this Agreement, IRIS Connect grants you a limited, non-exclusive, revocable licence (during the term of the Agreement) to use the Software and its accompanying documentation solely in connection with accessing the System.

20.2 License to Access the System

Upon establishing a valid Account, and subject to your continued compliance with this Agreement, IRIS Connect grants you a limited, non-exclusive, revocable licence (during the term of the Agreement) to access the System.

20.3 Specific Restrictions

20.3.1 Any and all rights not expressly granted by IRIS Connect herein are reserved, and no license, permission or right of access or use not granted expressly herein shall be implied.

20.3.2 You may not intercept, for any purpose, information accessible through the System. You may not access the System or upload, download or use information accessible through the System, other than as permitted by this Agreement.
20.3.3 You may not copy (except as set forth above), distribute, rent, lease, loan, modify or create derivative works of, adapt, translate, perform, display, sublicense or transfer the Software or any documentation accompanying the Software.

20.3.4 You may not reverse engineer, disassemble or decompile, or attempt to reverse engineer or derive source code from, all or any portion of the Software, or from any information accessible through the System (including, without limitation, data packets transmitted to and from the System over the Internet), or anything incorporated therein, or analyze, decipher, "sniff" or derive code (or attempt to do any of the foregoing) from any packet stream transmitted to or from the System, whether encrypted or not, or permit any third party to do any of the same, and you hereby expressly waive any legal rights you may have to do so. If the Software and/or the System contains license management technology, you may not circumvent or disable that technology.
20.3.5 You will not copy or create derivative works of the IRIS Connect platform, associated technology, learning programmes or other content resources that it hosts.

21. Proprietary Rights

21.1 Ownership of Software & System

As between you and IRIS Connect, IRIS Connect is the sole and exclusive owner of the Software & System. The Software & System are protected by law governing copyrights, trademarks and other proprietary rights. IRIS Connect reserves all rights not expressly granted herein. The System is comprised of, without limitation, software code, programs, routines, subroutines, objects, files, data, video, audio, text, content, layout, design and other information downloaded from and accessible through the System. . IRIS Connect, its affiliates, licensors and/or suppliers retain all of their right, title and interest (including without limitation all intellectual property rights) in and to the Software & System, and no rights thereto are transferred to you, except for the limited license granted above. IRIS Connect reserves the right to change service provider and/or software as long as the service provision is the same or better.

21.2 Rights to Certain Content

All recordings created through your account, are the sole and exclusive property of your Organisation, including any and all copyrights and intellectual property rights in or to any and all of the same, all of which are hereby expressly reserved

21.2.1 Non video data contributed by your Users to the programmes of third party providers will be treated in line with your service agreement with the third party provider

21.3 User Content

21.3.1 The System may allow you to communicate information, such as by sharing video & comments text, audio & video to group libraries (collectively, User Content).

21.3.2 User Content that you cause to be communicated to the System may not;

21.3.2.1 violate any statute, rule, regulation or law;

21.3.2.2 infringe or violate the intellectual property, proprietary, privacy or publicity rights of any third party;

21.3.2.3 be defamatory, indecent, obscene, child pornographic or harmful to minors; or

21.3.2.4 contain any viruses, Trojan horses, disabling code, worms, time bombs, "clear GIFs," cancelbots or other computer programming or routines that are intended to, or which in fact, damage, detrimentally interfere with, monitor, intercept or expropriate any data, information, packets or personal information.

21.3.3 IRIS Connect may take any action it deems appropriate regarding any User Content, if IRIS Connect believes, in its sole discretion, that such User Content violates this Agreement or may expose IRIS Connect, its licensors and/or its suppliers to liability, damage IRIS Connect's relationship with any of its suppliers, licensors, ISPs or other Users of IRIS Connect, harm anyone or IRIS Connect's reputation or goodwill.

21.3.4 Violation of IRIS Connect's proprietary rights is a material breach of this Agreement, in the event of which IRIS Connect may suspend your Account, terminate this Agreement and take whatever additional action IRIS Connect deems appropriate under the circumstance. The foregoing is without prejudice to or waiver of any and all of IRIS Connect's other rights and remedies, all of which are expressly reserved, survive termination, and are cumulative.

22. Warranties

22.1 The Software and System are provided "As Is," with all faults, and without warranty of any kind.

22.2 Where IRIS Connect relies on third party software to provide its service (such as operating systems and web browsers) IRIS Connect does not provide any warranties or guarantees that all operating systems or browsers will be supported, nor that hardware provided will be supported beyond the initial licence period.

22.3 To the extent permitted by law and save as expressly provided herein, IRIS Connect disclaims all warranties, whether express or implied, including without limitation the warranties of merchantability, fitness for particular purpose and non-infringement. IRIS Connect does not warrant that the operation of the System or access to the System, or that use of the Software, will be uninterrupted or error-free, nor that the System or Software will be compatible with the Organisation's hardware and software.

22.4 While IRIS Connect attempts to have the System available at most times, IRIS Connect does not guarantee that the System will always be available, or that the System will not become unavailable during use. The System may become unavailable for a number of reasons, including without limitation during the performance of maintenance to the System, for the implementation of new software, for emergency situations and due to equipment or telecommunications failures.

22.5 IRIS Connect warrants and represents that it shall comply with all applicable laws, statutes, regulations, directives, codes of practice and other analogous guidelines relevant to the Software and the System, including but not limited to those relating to anti-bribery and anti-corruption (such as the Bribery Act 2010).

22.6 The Organisation may terminate this contract and take action to recover all its losses if IRIS Connect commits an offence under the Bribery Act 2010 or Section 117(2) of the Local Government Act 1972 (as amended from time to time). Any clause limiting the IRIS Connect's liability does not apply to this anti-corruption clause.

22.7 During the term of this agreement and for a period of at least three years thereafter, IRIS Connect shall maintain in force, with a reputable insurance company, appropriate insurances to cover its liabilities, including public liability insurance, employer's liability insurance in an amount not less than £1,000,000 and shall, on the Organisation's request, produce both the insurance certificate giving details of cover and the receipt for the current year's premium.

23. Disclaimer of Damages

23.1 In no event shall IRIS Connect, its affiliates, licensors or suppliers be liable to you or to any third party for any special, indirect, incidental, consequential, punitive or exemplary damages (including without limitation, lost profits or lost data), arising out of or in connection with your Account, the System, Software, User Content, this Agreement, or any other services or materials provided in connection therewith, whether based on warranty, contract, tort or any other legal theory, and whether or not IRIS Connect is advised of the possibility of such damages, and even if any stated remedy fails of its essential purpose.

23.2 In no event shall the Customer, its affiliates, or suppliers be liable to IRIS Connect or to any third party for consequential damages, arising out of or in connection with your Account, the System, Software, User Content, this Agreement, or any other services or materials provided in connection therewith, whether based on warranty, contract, tort or any other legal theory, and whether or not the Customer is advised of the possibility of such damages, and even if any stated remedy fails of its essential purpose.

24. Limitation of Liability

24.1 Except as set forth below, IRIS Connect's and the Customer's maximum liability for any and all claims arising out of or in connection with this Agreement , shall not exceed an amount equal to the value of your current subscription fees.

24.2 In the event of a material breach IRIS Connect's obligations to provide access to and use of your Account, the System, or User Content, your sole and exclusive remedy shall be a refund of any pre-paid subscription fees attributable to the period during which you were denied such access and use.

24.3 If any of the foregoing disclaimers or limitations of liability are declared to be void or unenforceable, then IRIS Connect's liability shall be limited to the maximum extent permissible under applicable law. The remedies set forth herein are exclusive and in lieu of all other remedies, oral or written, express or implied.

25. Indemnity

25.1 The Organisation shall defend, indemnify and hold harmless IRIS Connect and its respective employees, officers and directors, from any and all claims, loss, damages and demands, including reasonable legal fees, arising out of the Organisation's (including its Users) use or misuse of the Software and/or System.

25.2 IRIS Connect shall defend, indemnify and hold harmless this Agreement and its respective employees, governors, agents and officers from any and all claims, loss, damages and demands, including reasonable legal fees, arising out of IRIS Connect's breach of this Agreement, including;

> **25.2.1** any damage to any third party property or for personal injury caused by IRIS Connect's negligence;
>
> **25.2.2** any applicable data protection legislation;
>
> **25.2.3** any infringement of third party intellectual property rights; or
>
> **25.2.4** any breach of the applicable warranties under clause 20.

25.3 If the customer is subject to the UK's "Education and Skills Funding Agency's (ESFA)" the indemnity is limited to the amount stated in the handbook".

26. Amendments to this Agreement

26.1 IRIS Connect may, at its sole discretion, amend this Agreement from time to time. If this Agreement is amended, you will be asked to review the amended Agreement when you log into your Account, and to indicate and confirm your acceptance of the amended Agreement by clicking the "Accept" and/or "Confirm" buttons.

27. Governing Law & Exclusive Forum

27.1 This Agreement, and the rights and obligations of the parties hereto, shall be governed and construed by and in accordance with the laws of:
i) England & Wales for customers located in the UK, Oceania or anywhere else other than the EEA, Switzerland, or the US,
ii) Republic of Ireland for customers located in the EEA (including Switzerland)
iii) State of Delaware for customers located in the US

The Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods.

27.2 The sole and exclusive forum for resolving any controversy, dispute or claim arising out of or relating to the Agreement, or otherwise relating to any rights in, access to or use of the Software, System, User Content and/or the rights and obligations of the parties hereto, shall be the:
i) English Court for customers located in the UK, Oceania or anywhere else other than the EEA, Switzerland, or the US,
ii) Republic of Ireland Court for customers located in the EEA (including Switzerland)
iii) State of Delaware Court for customers located in the US

28. Miscellaneous

28.1 If any part of the Agreement is held invalid or unenforceable, that portion shall be construed in a manner consistent with applicable law to reflect, as nearly as possible, the original intentions of the parties expressed in the Agreement, and the remaining portions shall remain in full force and effect.

28.2 The Organisation shall comply with all applicable laws regarding your access to and use of the System, use of the Software, your access to your Account. Without limiting the foregoing, you may not download, use or otherwise export or re-export any part of the information accessible through the System or the Software except in full compliance with all applicable laws and regulations.

28.3 Except as otherwise provided herein, you may not assign or transfer the Agreement or your rights there under, and any attempt to do so is void. The Agreement, the subscription fees and payment terms as referenced therein, as each may be amended by IRIS Connect and IRIS Connect from time to time, sets forth the entire understanding and agreement between IRIS Connect and you with respect to the subject matter hereof. Except as provided above, or in a writing signed by both parties, the Agreement may not be modified or amended. No distributor, agent or employee of IRIS Connect is authorised to make any modifications or additions to the Agreement.

28.4 All notices to IRIS Connect required or permitted by the Agreement shall be by electronic mail at support@irisconnect.co.uk, unless stated otherwise in the Agreement.

SECTION 4: APPENDIX

Appendix A: Information about the Processing

1. Subject Matter

Professional development of staff and delivery of training

2. Duration of the Processing

The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

IRIS Connect will process the data controller's data until the data controller instructs for the data to be deleted or they stop being a customer.

3. Purpose of the Processing

The data processor will process Customer Personal Data submitted, stored, sent or received by the Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to the Customer in accordance with the Data Processing Agreement.

The purpose of the data processor's processing of personal data on behalf of the data controller is:

The collection, sharing and analysis of video and other associated content typically for professional development, delivery of training, capture of events, meetings and video calls

4. Nature of Processing

The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

- *Storage*
- *Processing (changing the format of the data into streamable and interactable formats).*
- *Recording or capture (videos/audio data) via screen capture, call recording, video call recording and videoing via dedicated apps*
- *Upload captured video data securely*
- *Adaption or Alteration e.g. clipping via editing feature*
- *Duplication e.g. via the copy/clone feature*
- *Annotation via the comment feature*

- *Organisation via the tagging feature*
- *Share to other approved Users accounts via the platform*
- *Erasure or destruction via the delete feature*
- *Retrieval and Dissemination e.g. enable streaming (playback of videos)*
- *Other processing include uploading of photos, files, text*
- *Creation of User accounts (containing name and email address, password and optional tags)*

5. Categories of Data

Personal data submitted, stored, sent or received by the Customer, its Affiliates or End Users via the Services may include the following categories of data:

- *Personal Data including Special category data*

The categories of data that are processed by IRIS Connect is determined by The Customer (the Data Controller), who decide what data to upload to the IRIS Connect platform.

IRIS Connect Platform data can be in the form of video recordings, audio recordings, username, user IDs, email address, users' full name, file uploads (documents, presentations), images, text and media comments, usage data, metadata, course, assignment or pathway progress and submitted answers, user and video 'tagging', form data (both text and quantitative) and other data.

6. Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of the Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Processing includes the following categories of data subject:

- *The data controller's employees, trainees, pupils, customers and service users*

The categories of data subject that are processed by IRIS Connect is determined by The Customer (the Data Controller), who decides what data to upload to the IRIS Connect platform.

Appendix B: Authorised Sub-processors

B.1. Approved sub-processors

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

NAME	BUSINESS NUMBER	DATA CENTRE	DESCRIPTION OF PROCESSING
Amazon AWS	390566 (Ireland) 91-1646860 (US) 30 616 935 623 18 (Australia)	EU West eu-west1 *Dublin, Ireland* US East us-east-1 *N. Virginia, USA* US West us-west-2 *Oregon, USA* Asia Pacific (Sydney) ap-southeast-2 *Sydney, Australia*	All data uploaded to the platform, including video, audio, screen capture, images, attachments, video conference hosting, comments are stored and processed on Amazon AWS servers. *See section 16.3 for which region customer's data is held*

Optional sub-processors

NAME	BUSINESS NUMBER	DATA CENTRE	DESCRIPTION OF PROCESSING
Microsoft Azure **The use of Azure as a**	GB639237322 (UK)	UK South *London, UK*	AI analysis of user submitted video content

sub-processor only applies to our customers that use AI Insights feature	556952-8150 (Sweden) 91-1144442 (US) 29 002 589 460 (Aus)	Sweden Central, *Gävle, Sweden* US East *Richmond, USA* Australia East *New South Wales, Australia*	
OpenAI **The use of Azure as a sub-processor only applies to our customers that use AI Insights feature**	7063675 (US)	US	AI analysis of user submitted video content
OVH **The use of OVH as a sub-processor only applies to our customers that have opted-in to using the Rooms (video conferencing) feature**	5519821 (UK) 537 407 926 (France)	Erith, London, England Roubaix, Paris, France	Video conferences are hosted on OVH servers. Video conference recordings are created on OVH servers before being immediately transferred to Amazon servers and removed from OVH. *Server location used that is appropriate for your local data protection law*
Twilio **The use of Twilio as a sub-processor only applies to our customers that have opted-in to using**	4518652 (US)	375 Beale St #300, San Francisco, CA, US	Phone call recordings are created on the Twilio server during the call before being immediately transferred to Amazon (see above) and removed from Twilio.

the call recording feature			

International Data Transfers

NAME	TRANSFER TYPE	DATA TRANSFER	METHOD
AWS	UK data transfer to EU	Customer video data	Adequacy decision
OpenAI Optional feature	UK data transfer to US EU data transfer to US	Customer video data	EU: EU SCCs or Adequacy Decision - See Appendix D UK: UK addendum to the EU SCCs - See Appendix E
Twilio Optional feature	UK data transfer to US EU data transfer to US	Customer call recordings	EU - EU SCCs - See Appendix D UK: UK addendum to the EU SCCs - - See Appendix E

Appendix C: Instruction Pertaining to the Use of Personal Data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The IRIS Connect system enables Users to perform the following actions to their data

- *Capture (videos/audio data) via screen capture, call recording, video call recording and videoing via dedicated apps*
- *Upload captured video data securely*
- *Store securely*

- *Clip (via editing feature)*
- *Copy*
- *Comment and tag*
- *Share to other approved Users accounts via the platform*
- *Delete*
- *Stream (playback videos)*
- *Other processing include uploading of photos, files, text*
- *Creation of User accounts (containing name, email address, password and optional tags)*

All these instructions are able to be given directly via the IRIS Connect Web Platform. All standard processing by IRIS Connect is carried out automatically via the system.

C.2. Security of processing

The level of security shall take into account:

The processing involves a large volume of personal data, and therefore a high level of security should be established."

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Storage Redundancy

Hourly backups of database
Save data to multiple availability zones within the region.
Verify the integrity of the data using checksums, automatically repairing any data inconsistencies

Destruction of Data

Customer data (financial) shall be retained in line with local legal frameworks. Customer data (non-financial) shall be securely disposed of and/or transferred to the client following termination of licence.
Data that the client instructs to be destroyed will be stored in 3 months. The back-ups will be stored in 3 months.
There are certain occasions when information needs to be preserved beyond this limit, such as in the following circumstances:
Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual
A crime is suspected or detected

The highest standard of industry procedure shall be used when decommissioning of storage devices at the end of their useful life.

Secure encryption

IRIS Connect must ensure that any data in transit is encrypted using TLS. Additionally, data stored on mobile devices shall be encrypted while stored to ensure that data is protected before it enters a secure cloud service.

Organisational security

IRIS Connect shall, in line with GDPR and ISO27001 recommendations, regularly review its organisational and cyber security and has comprehensive information security processes and protocols.

Service Level

IRIS Connect shall utilise market leading services for data processing and storage.
IRIS Connect shall provide free full support to all customers
The support team shall be available via live chat, email and phone.

Authorisation and access control

IRIS Connect shall ensure that User role separation and permissioning governs access to appropriate data and features.
The IRIS Connect system shall be based on individual User accounts and permissioning. Meaning that the observed User has to agree to a recording taking place before the system allows another User to connect to the camera. The same protection shall exist once a video has been encrypted and uploaded. This means Users are only able to see data that has been explicitly shared with them. By default Users shall be limited to sharing videos with other Users at their organisation.
Users shall have complete control over who has access to their data by deciding to share videos either with individual Users or into a group library. A fundamental principle of the system is that Users will never "lose sight or control" of their video. They shall always be able to see the video and any associated data.
Users retain the right to delete a video or remove sharing privileges at any time.
IRIS Connect staff may access customer data for the sole purpose of fulfilling our obligations to the data processor. All access to data is carefully performed following secure processes and procedures.

Input data that contains personal data

Only the data owners shall have access to the data at input stage. Users are responsible for input into the system, and data can only be input into Users' specific account with the confidential password and unique Username.
IRIS Connect Equipment does not permanently store files locally.
For full User control and data security, videos shall never be stored on individual devices or local servers. Instead, they shall be encrypted, immediately uploaded to the IRIS connect platform and automatically deleted from the device they were recorded on.

The platform shall be designed to ensure that data remains in the secure, password protected environment. The deletion of the input data by a User shall be managed via an automated process build into the design of the system

Output data that contain personal data

The IRIS Connect system shall be based on individual User accounts and permissioning, where each User has their own personal Username and password for their account in the IRIS connect platform. The observed User has to agree to a recording taking place before the system allows another User to connect to the camera.
The same protections exist once a video has been encrypted and uploaded. This means Users shall only be able to see data that has been explicitly shared with them. Users shall be limited to sharing videos with other Users at their organisation, or collaboration with other organisations if this has been enabled with the permission of the Organisation Administrator. All data shall be securely stored and can only be delivered to the User via an encrypted channel.
The organisation and its Users shall be in complete control of their data, so IRIS connect will only destroy data upon the instruction of the data controller.
If the data is deleted by the owner, deleted data shall be stored for 3 months in case the customer needs to retrieve it. The back-ups shall be stored for 3 months before being securely and automatically destroyed to ensure that it cannot be misused or accessed by unauthorised persons

External communication connections

The IRIS Connect system shall be fully cloud-based and designed to ensure that unauthorised persons cannot gain access to data. IRIS Connect shall ensure any data in transit is encrypted using TLS.. Any data removed from our secure system shall be done so under authorisation of the data controller or by authorised personnel for the purpose of data processing.

Control of rejected access attempts

The IRIS Connect platform shall log every account login attempt. The system shall also block repeated login attempts to the same account within a determined time period, by locking the User's account until this is reviewed by an authorised person.

Logging

IRIS Connect shall collect comprehensive User activity logs that are stored for six months.

Home offices

IRIS Connect shall not permit and physically restrict data processing at home including holding data locally, or printing data locally. All data shall be held securely within the IRIS connect cloud-based system.

Privacy by design

IRIS Connect shall be constructed with privacy-by-design principles at its core.

Appendix D: Standard Contractual Clauses

NOTE- Only for EEA-based customers using either the:

1) AI Insights feature with OpenAI

2) Call Recording feature

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

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 these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject

shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the

supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant

information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Republic of Ireland for customers located in the EEA (including Switzerland)

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Republic of Ireland for customers located in the EEA (including Switzerland)

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: *Customer*

Address: *N/A*

Contact person's name, position and contact details: *N/A*

Activities relevant to the data transferred under these Clauses:

Creation and transfer of data to data processor

Signature and date:

Role (controller/processor): *Data Controller*

2.

Name: *IRIS Connect Ireland*

Activities relevant to the data transferred under these Clauses:

Processing of data and transfer to sub-processor

Signature and date:

Role (controller/processor): *Data Processor*

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.

Name: *OpenAI*

Address: *3180 18th Street, San Francisco, California 94110, United States*

Contact person's name, position and contact details: *N/A*

Activities relevant to the data transferred under these Clauses: *AI analysis of video/transcript*

Signature and date: *N/A*

Role (controller/processor): *Sub-Processor*

2.

Name: *Twilio*

Address: *375 Beale St #300, San Francisco, CA, US*

Contact person's name, position and contact details: *N/A*

Activities relevant to the data transferred under these Clauses: *Processing of call recording data*

Signature and date: *N/A*

Role (controller/processor): *Sub-Processor*

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- *Employees of the customer (teachers & staff)*
- *Service users of the customer (pupils attending the education institution)*

The categories of data subject that are processed is determined by The Customer (the Data Controller), who decides what data to upload to the IRIS Connect platform.

Categories of personal data transferred

- *Personal Data including Special category data*

The categories of data that are processed is determined by The Customer (the Data Controller), who decide what data to upload to the IRIS Connect platform

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

OpenAI: *Analysis*

Twilio: *Processing*

Purpose(s) of the data transfer and further processing

Professional development

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

OpenAI*:30 days*

Twilio*: Data is immediately transferred to Amazon upon completion of the call. Data is then deleted from Twilio*

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described above

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Data Protection Comission: Ireland

ANNEX II

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

OpenAI & Twilio:

- *Data access restriction - limited to the engineering team and the end user*
- *Minimal data retention periods*
- *Automated event logging for audit trails*
- *OpenAI security review conducted*
- *Data is transmitted over an encrypted TLS connection*

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

As described above

...

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. **Name**: *OpenAI*

   Address: *3180 18th Street, San Francisco, California 94110, United States*

   Contact person's name, position and contact details: *N/A*

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): *AI analysis of video/transcript*

2. **Name**: *Twilio*

   Address: *375 Beale St #300, San Francisco, CA, US*

   Contact person's name, position and contact details: *N/A*

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): *Processing of call recording data*

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Appendix E: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

NOTE- Only for UK/Oceania-based customers using either:

1) AI Insights feature with OpenAI

2) Call Recording feature

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	03/06/2024		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: IRIS Connect LTD Trading name (if different): IRIS Connect Main address (if a company registered address): IRIS Connect, Unit 3, Adur Dock 104 Albion Street, Southwick, Brighton, BN42 4DP Official registration number (if any) (company number or similar identifier): 06444348	Full legal name: OpenAI L.L.C Trading name (if different): OpenAI Main address (if a company registered address): 3180 18th Street, San Francisco, California 94110, US Official registration number (if any) (company number or similar identifier): 7063675	Full legal name: Twilio Inc. Trading name (if different): Twilio Main address (if a company registered address): 375 Beale St #300, San Francisco, CA, US Official registration number (if any) (company number or similar identifier): 4518652
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:

Signature (if required for the purposes of Section 2)			

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: 03/06/2024 Reference (if any): Other identifier (if any): IRIS Connect: Organisation Administrator & Data Processing Agreement v1.4

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Customer, IRIS Connect, OpenAI, Twilio

Annex 1B: Description of Transfer:

Categories of data subjects whose personal data is transferred:

Employees of the customer (teachers & staff)

Service users of the customer (pupils attending the education institution)

The categories of data subject that are processed is determined by The Customer (the Data Controller), who decides what data to upload to the IRIS Connect platform.

Categories of personal data transferred:

Personal Data including Special category data

The categories of data that are processed is determined by The Customer (the Data Controller), who decides what data to upload to the IRIS Connect platform.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis

Nature of the processing:

Analysis

Purpose(s) of the data transfer and further processing:

Professional development

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

OpenAI: 30 days

Twilio: Data is immediately transferred to Amazon upon completion of the call. Data is then deleted from Twilio

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

As described above

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

OpenAI & Twilio:

Data access restriction - limited to the engineering team and the end user

Minimal data retention periods

Automated event logging for audit trails

OpenAI security review conducted

Data is transmitted over an encrypted TLS connection

Annex III: List of Sub processors (Modules 2 and 3 only): *OpenAI, Twilio*

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ Neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection

Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data

Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.