IRIS Connect : Organisation Administrator & Data Processing Agreement

Table of Contents

1. Preamble

1.1 This is an agreement between you and the entity you represent ("Customer", "you" or "your") that for the purposes of this agreement will be acting as the Data Controller, and IRIS Connect / iConnect Ireland Limited ("IRIS Connect") that 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 dataprocessor, 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 Connect 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 Section 4 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 Section 4 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 Section 4 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 Section 5 details the Standard Contractual Clauses (SCCs). These are standard sets of contractual terms and conditions which the sender (controller) and the receiver (processor) of the personal data both sign up to. They include contractual obligations which help to protect personal data when it leaves the EEA and the protection of GDPR.

1.10 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 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 Data Protection Legislation**” means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

“**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 in which the data controller is established;

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

“**Security Documentation**” means all documents and information made available by IRIS Connect under Clause 10 and on our website

“**Security Measures**” has the meaning given by IRIS Connect’s Security Measures and Controls document.

“**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 authorized 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.

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 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. 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 accept 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 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 the group is created by your organisation 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

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 seek advice to be absolutely certain that the circumstances warrant using 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 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 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 will monitor all future rulings that may affect these agreements and commit to altering them or making any additional provisions required of any clear ruling, within this specified time frame given within the ruling, or 3 months, whichever is shorter.

5.4 Application of European Legislation.
The parties acknowledge and agree that the European Union 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 EEA; and/or
5.4.2 The Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

5.5 Non European Union Data Controllers
For data controllers located outside of the European Union, IRIS Connect commits to process your data in accordance with your Local Regulatory Framework.

5.6 Processor and Controller Responsibilities.
If the European Union 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 Data Protection Legislation;
5.6.3 The Customer is a controller or processor, as applicable, of that Customer Personal Data under the European Union 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 another processor, have been authorized 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.

5.12 The Standard Contractual Clauses listed in Section 4 will only apply to Data Controllers to which the GDPR is in force.

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 where the data controller is established) and does not violate the relevant provisions of that State. 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 will provide 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 Union or Member State law to which the processor is subject. 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; 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;

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.

7.3 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:

7.3.1 to provide the Services and related technical support;
7.3.2 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;
7.3.3 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.

7.4 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.

7.4.1 IRIS Connect will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services.
7.4.2 IRIS Connect does not allow any third parties to view or modify customer data outside of the purpose of providing the contracted services.

7.5 Impact Assessments and Consultations
The Customer agrees that 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:

7.5.1 providing the Additional Security Controls in accordance with Section 10 (Security of Data Processing) and the Security Documentation
7.5.2 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 instructs 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.

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 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 necessary 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 organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized 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 authorized to process Customer Personal Data 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 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.
The Customer agrees that 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, details of the Data Incident, including steps taken to mitigate the potential risks and steps IRIS Connect recommends the Customer take to address the Data Incident.

11.3 Delivery of Notification.

Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at IRIS Connect's discretion, 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.

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

12.1.2.3 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), or 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 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 the DfE Cloud Service Providers self certification
12.6.2 maintain Cyber Essentials (or higher) certification
12.6.3 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 certificate

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

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 review of the Security Measures and Controls document and/or audit. 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:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

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 Australia 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 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.

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:

a. transfer personal data to a data controller or a data processor in a third country or in an international organization
b. transfer the processing of personal data to a sub-processor in a third country
c. 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 19.7 (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 same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU law or relevant state law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the 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 his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

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. 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;
19.5.2 in a notice on IRIS Connect's website;
19.5.3 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.

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;
19.8.3 you or anyone using any of your Account materially breaches this Agreement, makes any unauthorized 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. 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. 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 the 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
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.

19.9.3.1 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 license 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 license to access the System.

20.3 Specific Restrictions

20.3.1 Any and all rights not expressly granted by IRIS Connect and 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 (collectively, "RIS Connect "). 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 your Account, the Software, User Content, the Agreement, and any other services or materials provided in connection therewith, shall not exceed an amount equal to the value of your current subscription fees.

24.2 In the event of a material breach of IRIS Connect and 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

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 the Republic of Ireland. 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 Court of Republic of Ireland.

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 authorized 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.

Updated: 3rd November 2020
Version 0.3

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: User IDs, email, documents, presentations, images, calendar entries, tasks and other data.

- *Personal Data including Special category 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*

Appendix B: Authorised Sub-processors

B.1. Approved sub-processors
On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	BUSINESS NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Amazon AWS*	390566 (Ireland) 91-1646860 (US) 30 616 935 623 18 (Australia)	Greenhills Road, Tymon North, Dublin, Ireland 21155 Smith Switch Road, Ashburn, VA, USA. 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.
OVH**	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.
Call Recording (Optional feature) **The use of Twilio as a sub-processor only applies to our customers that have opted-in to using our phone call recording service.**			
Twilio***	26-2574840 (US)	375 Beale St #300, San Francisco, CA, US Data sharing covered by binding corporate rules (BCR)	Phone call recordings are created on the Twilio server during the call before being immediately transferred to Amazon (see above) and removed from Twilio.

** See section 16.3 for which customer's data is held where*
*** Server location used that is appropriate for your local data protection law*
**** For more information about the use of Twilio see our GDPR page*

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.

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 the leading industry practice (TLS 1.2). 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.

Authorization 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 organization.

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 the leading industry practice (TLS 1.2). 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.

SECTION 5: STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS FROM CONTROLLER TO PROCESSOR

Clause 1. Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [1]

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation 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 Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting 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.

Clause 2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3. Third-party beneficiary clause

(1) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

(2) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

(3) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

(4) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) 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 Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) 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;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, 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 Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 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 importer under the Clauses;

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5. Obligations of the data importer [2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) 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;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter 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 exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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 exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6. Liability

(1) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

(2) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

(3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7. Mediation and jurisdiction

(1) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

(2) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8. Cooperation with supervisory authorities

(1) The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

(2) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

(3) The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9. Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11. Sub-processing

(1) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[3]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

(2) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

(3) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

(4) The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12. Obligation after termination

(1) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

(2) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Additional commercial clauses

Priority of standard contractual clauses

The Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Clauses are entered into.

Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect.

Effective date of the Standard Contractual Clauses

The parties intend that these Clauses should only become effective if Art 44 of the General Data Protection Regulation (the "GDPR") applies to a transfer of personal data from the EEA to the UK, because the UK has left the European Union, and the transfer is not permitted under Art 45.

On that basis, the Clauses will become effective on:

(i) the first date Article 44 GDPR applies to a transfer of personal data from the EEA to the UK, and that transfer is not permitted under Article 45 GDPR; or

(ii) the date of the Standard Contractual Clauses, if later.

In this clause, 'a transfer of personal data' has the same meaning as in Article 44 of the GDPR.

Appendix 1

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

- Education

The data exporter's business or organisation type is:

- Education

The data exporter is using the personal data which is being transferred for the following purposes or activities:

- Education, including the provision of education or training as a primary function or as a business activity.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

The data importer's business or organisation type is:

- Education

The data importer’s activities for the data exporter, which are relevant to the transfer are:

- IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff.

- Customers and clients (including their staff)

Categories of data

The personal data transferred concern the following categories of data:

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

- Not applicable

Processing operations

The personal data transferred will be subject to the following basic processing activities:

- Collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction

Appendix 2

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 measures that are detailed in Appendix C.2. (Security of processing).

Footnotes

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this clause if they considered it better for the contract to stand alone.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

[3] This requirement is satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this decision.