DATA PROTECTION POLICY

Document reference:	Data Protection Policy
Issue Number:	Issue
Issue Date:	See section 12.0
Review date:	12 months from approval date * please see section 12.0
Document Owner: (responsibility for keeping the document up to date):	Compliance Manager
Version Control inc. approval status):	Via SharePoint - This is a controlled document. Any printed copies of this document are deemed uncontrolled.

Preface

ONVU Technologies AG (OVT) and its subsidiaries and affiliates deliver video and data-led technology solutions through annual investment in R&D, talent acquisition and partnerships, to enable our global partners and customers to make informed business choices across the surveillance, education, and retail sectors.

For simplicity throughout this policy, 'we' and 'us' means OVT and its subsidiaries and affiliates.

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The EU General Data Protection Regulation entered into force across the European Union (which at the time included the UK) in 2018, replacing the EU Data Protection Directive of 1995. The GDPR's broad purpose is to protect the "rights and freedoms" of natural persons (i.e., living individuals) and to ensure that personal data is not processed without their knowledge and that it is otherwise processed fairly and lawfully.

Throughout this policy where we refer to the GDPR this encompasses the UK GDPR unless otherwise stated.

When the UK fully left the European Union, the 'UK GDPR' (read in conjunction with the UK Data Protection Act 2018) replaced the GDPR in the United Kingdom. Whilst the two laws may diverge in the future for the time being they are substantively the same. As such, the regulatory guidance, case law and other business practices that have developed since 2018 remain relevant and protecting personal data remains at the heart of UK data protection law.

The GDPR is a principles-based regime. This means that to process data compliantly, an organisation should always aim to follow the underlying principles and that this is just as important as following, where applicable, the GDPR's more prescriptive rules. OVT adopts UK GDPR as a foundational set of principles when setting about applying processes to other territories until those territories' equivalents are met. This is on the basis that most data processed for the purpose of OVT operations is UK based. If, for example, an AWS instance is used for data processing in a different territory then that territory's data protection rules apply if different. The GDPR principles are set out in section 4 of this policy.

1.2 Definitions used by OVT

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (e.g., by computer) and to the processing other than by automated means of personal data (e.g., paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) –The definition of Data Controllers and Processors and their respective responsibilities is taken as being as defined within the relevant territories such as UK GDPR (or territorial equivalent) legal framework.

Data protection framework – Throughout this policy as well referring to data protection law, we also refer to jurisdiction's (which may be the UK ,EU Member State, US and or UAE etc.) 'data protection legal framework. This definition includes the legal requirements, but also relevant guidance and codes of practice issued by regulatory authority (for example, the Information Commissioner's Office or 'ICO' in the UK). Please also refer to section 10. Data Transfers.

1.3 Definitions taken directly from the GDPR (and most found in Article 4 of the GDPR)

Main establishment – the main establishment of the controller in the UK will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the UK will be its administrative centre. If a controller or processor is based outside the UK, it may have to appoint a representative in the jurisdiction in which the controller or processor operates to act on behalf of the controller or processor and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and criminal offence data.

Data controller – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
The controller has overall responsibility for processing personal data even if it asks a data processor to undertake certain processing activities on its behalf.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, store, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Consent – means any freely given, specific, informed, and unambiguous indication of the data subjects wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – Processing a child's personal data (noting that the definition of a child may vary across different jurisdictions) requires particular protection because children may be less aware of the risks involved. As with any individual, when a child's personal data is processed the controller must be able to identify a lawful basis for the processing. Consent is one possible lawful basis, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child. In the case of OVT's customers (who, as controllers, will have overall responsibility for any processing undertaken using our solution), the lawful basis is likely to be public interest in the performance of the school's statutory functions.

OVT, specifically the ONVU Learning division, recognise that children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved. OVT commits to complying with all the requirements of the relevant territory's data protection legal framework to minimise and mitigate risks. ONVU Learning, in addition, recognises that:

- As a processor of children's personal data via our ONVU Learning Product we ensure that we are always mindful of that at the forefront of the planning and design of our systems, product, and processes. Compliance with the data protection principles and in particular fairness will be central to all our processing of children's personal data.
- ONVU Learning will generally process recorded video and audio data under the lawful basis of legitimate interests and if processes data for any other lawful basis this will be recorded and where appropriate explained to the individuals involved.
- It is the customers responsibility to ensure that whoever has parental responsibility for the child ensures permission is gained if the customer intends to use any imagery for purposes other than those outlined in our user agreements.
- OVT will never use a child's personal data for marketing purposes or creating personality or user profiles. Anonymised data may be used to improve our processes and systems.
- OVT recognise that children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- We ensure that our processing is fair and complies with the data protection principles.
- As a matter of good practice, ONVU Learning provide exemplar templates to customers for them to develop DPIAs to help us assess and mitigate the risk.

Third party – a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2.0 Data Protection Policy Statement

2.1 The Board of Directors and management of OVT, of: PostStrasse 14, 6300, Zug, Switzerland, are committed to compliance with, and the protection of the "rights and freedoms" of individuals whose information OVT collects and processes in accordance with the GDPR.

2.2 Compliance with UK GDPR's and associated legislation is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures. All associated policy, process and or procedure are detailed within OVT information management system, summarised in 3.2.2.

2.3 The GDPR and this policy apply to all of OVT 's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes.

2.4 OVT has established objectives for data protection and privacy, which are detailed within the ~~data~~ information management system.

2.5 The Compliance Manger is responsible for reviewing the data inventory of processing annually in the light of any changes to OVT 's activities as determined through; changes to the data retention schedule, management review, audit results and to any additional requirements identified by means of data protection impact assessments or indeed changes to legislation. This schedule will be made available to the Information Commissioner's Office's (ICO) or equivalent territorial supervisory authority upon request.

2.6 This policy applies to all Employees/Staff and third parties and interested parties as authorised by OVT such as outsourced suppliers. Any breach of the GDPR or this management system will be dealt with through OVT 's disciplinary policy. Moreover, in certain specific circumstances, infringement of the GDPR by an organisation and/or a specific individual may amount to a criminal offence. In the unlikely event that this occurs, OVT will take all appropriate and necessary action, including notifying the relevant authorities, in the applicable territory where the criminal offence took place .

2.7 Partners and any other third parties working with or on behalf of OVT, and that have or may have access to personal data, will be expected to have read and understood this policy, and to comply with it.

No third party may access personal data held by OVT without having first entered into a data confidentiality agreement and or contract detailing the third parties' expectations in relation to data protection which will impose on the third-party obligations no less onerous than those to which OVT are committed, and which gives OVT the right to audit compliance with the agreement or contract.

3.0 Information management system (SYSTEM)

3.1 Information Management System Policy Statement

To support compliance with the GDPR, the Board of Directors has approved and supported the development, implementation, maintenance, and continual improvement of a documented (data) information management structure (or 'system') for OVT.

All Employees/Staff of OVT and certain external parties identified within the system are expected to comply with this policy and with the system which implements this policy. All Employees/Staff, and certain external parties, will receive appropriate and proportionate training.

The consequences of breaching this policy are set out in OVT 's disciplinary policy and in contracts and agreements with third parties.

3.2 Scope

In determining the scope for compliance with the system it shall cover all OVT affiliates and subsidiaries' data which is personally identifiable information which the organisation holds, including data that is shared with external organisations such as suppliers and cloud service providers. The system also takes into consideration any transfer of data to other countries, as applicable, and the processing functions undertaken on behalf of our customers.

3.2.1. OVT considers:

- Any external and internal issues that are relevant to the purpose of OVT and that affect its ability to achieve the intended outcomes of its system;
- Specific needs and expectations of interested parties that are relevant to the implementation of the system;
- Organisational objectives and obligations;
- The organisation's acceptable level of risk; and
- Any applicable statutory, regulatory, or contractual obligations.

3.2.2 OVT 's objectives for compliance with the GDPR and our management systems:

- Are consistent with this policy;
- Are measurable;
- Take into account the results from risk assessments and risk treatments;
- Are monitored (in line with the Monitoring, Measurement, Analysis, Evaluation Procedure);
- Are communicated (in line with the Communications Procedure); and
- Are updated as appropriate in line with continual improvement.

3.2.3 OVT commits to documenting those objectives.

3.3 In order to achieve these objectives, OVT has determined:

- What will be done
- What resources will be required
- Who will be responsible
- When it will be completed

- How the results will be evaluated

3.4 Responsibilities and roles under the GDPR

3.4.1 OVT is both a data controller and a data processor (in relation to different processing activities) under the GDPR definitions detailed in Articles 24, 26, 27, 28 and 29.

3.4.2 Top Management and all those in managerial roles throughout OVT are responsible for developing and encouraging good information handling practices within OVT; responsibilities are set out in individual job descriptions.

3.4.3 The Compliance Manager supported by the Executive Team is the accountable GDPR owner for OVT and for the subsequent management of personal data within OVT and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.4.3.1 Development and implementation of the GDPR as required by this policy;
3.4.3.2 Security and risk management in relation to compliance with the policy; and
3.4.3.3 Development, implementation and training for the information management system and its components.

3.4.4 The Compliance Manager, who the Board of Directors considers suitably qualified and experienced, has been appointed to take responsibility for OVT 's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that OVT complies with the GDPR, as do Employees/Staff in respect of data processing that takes place within their area of responsibility.

3.4.5 The Compliance Manager has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.4.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of OVT who process personal data.

3.4.7 OVT 's Data Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of OVT generally.

3.4.8 Employees/Staff of OVT are responsible for ensuring that any personal data about them and supplied by them to OVT is accurate and up to date.

4.0 Data protection principles

4.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. OVT 's policies and procedures are designed to ensure compliance with these principles.

4.2 Personal data must be processed lawfully, fairly, and transparently.

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14.

These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. OVT will ensure that this is communicated to data subjects in an intelligible form using clear and plain langue.

Providing accessible information to individuals about the use of their personal information (data) is a key element of their legal right to transparency as set out in the UK General Data Protection Regulation (UK GDPR). OVT sets out the requirements for the provision of the organisations privacy notices in a dedicated Privacy Procedure. Privacy Notices are displayed as applicable, whether on our websites, internal employee notices or product such as the ONVU Learning classroom video lesson observation systems and will be issued/displayed as applicable to data subjects. Please also see Section 5.0

Where acting as a data controller the specific information that OVT will provide to the data subject will, as a minimum, include:

4.2.1 The identity and the contact details of the controller and, if any, of the controller's representative;
4.2.2 The contact details of the person responsible for GDPR;
4.2.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.2.4 The period for which the personal data will be stored;
4.2.5 The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.2.6 The categories of personal data concerned;
4.2.7 The recipients or categories of recipients of the personal data, where applicable;
4.2.8 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data; and
4.2.9 Any further information necessary to guarantee fair processing.

4.3 Personal data can only be collected for specific, explicit, and legitimate purposes. Data must not be used for a purpose other than that for which the personal data was collected (other than where the data subject has consented or otherwise in accordance with applicable law). The Privacy Procedure sets out the relevant procedures.

4.4 Personal data must be accurate, relevant, and limited to what is necessary for processing.

4.4.1 The Compliance Manager, supported by departmental managers, is responsible for ensuring that OVT does not collect information that is not strictly necessary for the purpose for which it is obtained (this is achieved through the data flow/mapping).
4.4.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to a privacy statement, and be approved by the department managers, supported by the Compliance Manager.

4.4.3 The Senior VP for Compliance and Finance supported by the Compliance Manager will ensure that, on a regular basis, all data collection methods are reviewed by the Compliance Manager, supported by departmental managers, to ensure that collected data continues to be adequate, relevant, and not excessive.

4.5 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.5.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
4.5.2 The Compliance Manager is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
4.5.3 It is also the responsibility of the data subject to ensure that data held by OVT is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
4.5.4 Employees, staff, customers and third parties are required to notify OVT of any changes in circumstance to enable personal records to be updated accordingly It is the responsibility of OVT to ensure that any notification regarding change of circumstances is recorded and acted upon.
4.5.5 The Compliance Manager, supported by departmental managers, is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
4.5.6 On at least an annual basis, OVT will review the retention dates of all the personal data processed by OVT, by reference to the data retention schedule, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Data Procedure (inc. Hardware).
4.5.7 The Compliance Manager is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure -SARS). This can be extended by a further two months for complex requests. If OVT decides not to comply with the request, we must respond to the data subject to explain its reasoning and inform them of their right to complain to the relevant supervisory authority and seek judicial remedy.
4.5.8 The Compliance Manager is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.6 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.6.1 Where personal data is retained beyond the processing date, it will be anonymised in order to protect the identity of the data subject in the event of a data breach.
4.6.2 Personal data will be retained in line with the Data Retention Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
4.6.3 The Senior VP for Compliance and Finance must specifically approve any data retention that exceeds the retention periods defined in the Data Retention Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.7 Personal data will be processed by OVT in a manner that ensures appropriate security and will; consider the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. Those measures shall be reviewed and updated where necessary.

4.8 The Compliance Manager, supported by departmental management, will carry out a risk assessments considering all the circumstances of OVT 's controlling and or processing obligations and operations.

4.8.1 In determining appropriateness, the Compliance Manager, supported by departmental managers, shall also consider the extent of possible damage or loss that might be caused to individuals (e.g., staff or customers) if a security breach occurs, the effect of any security breach on OVT itself, and any likely reputational damage including the possible loss of customer trust.

4.8.2 When assessing appropriate technical measures, the Compliance Manager and IT manager will consider the following protocols:

- Password protection (IT Access Control Policy)
- Automatic locking of idle terminals.
- Removal of access rights for USB and other memory media (IT Access Control Policy and Secure Disposal of Data Procedure inc Hardware).
- Virus-checking software and firewalls
- Role-based access rights including those assigned to temporary staff (IT Access Control Policy)
- Applied principle of least privilege
- Encryption of devices that leave OVT 's premises such as laptops
- Security of local and wide area networks (Information Security Policy)
- Privacy enhancing technologies such as pseudonymisation and anonymisation.
- Identifying appropriate international security standards relevant to OVT.

When assessing appropriate organisational measures, the Compliance Manager and IT manager will collectively consider;

- The appropriate training levels throughout OVT;
- Measures that consider the reliability of employees (such as references, DBS checks etc);
- Including data protection in employment contracts;
- Identifying disciplinary action measures for data breaches;
- Monitoring staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employees' own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site; and
- Imposing contractual obligations on the importing organisations to take appropriate security measures if transferring data outside the EEA.

4.8.3 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. OVT may appoint the services of third-party specialist to test and verify any vulnerability, actual or potential, concerns to mitigate any loss, damage or distress to data subjects.

4.9 OVT are able to demonstrate compliance with GDPR's principle of accountability. The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires OVT to demonstrate that we comply with the principles and explicitly states our responsibility.

4.10 OVT will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, and adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5.0 Data subjects' rights

5.1 OVT fully understand that data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 The right to be informed when their personal data is being processed.
5.1.2 The right to access personal data held about them, including the nature of information held and to whom it has been disclosed.
5.1.3 The right to have processing restricted in certain cases.
5.1.4 The right to prevent processing for purposes of direct marketing.
5.1.5 The right to be informed about the mechanics of automated decision-making processes that will significantly affect them.
5.1.6 The right to not have significant decisions that will affect them made solely by automated process.
5.1.7 The right to sue for compensation if they suffer dame by any contravention of the GDPR.
5.1.8 The right to have personal data rectified or erased and to block processing of personal data.
5.1.9 The right to object to processing in specific instances.
5.1.10 The right to request the supervisory authority to assess whether any provision of the GDPR has been contravened.
5.1.11 The right to have personal data provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller.
5.1.12 The right to object to any automated profiling that is occurring without consent.

5.2 OVT ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data subject access requests (SARs) (along with all other applicable rights, although SARs are the most commonly exercised right) as described in the Subject Access Request Procedure; this procedure also describes how OVT will ensure that its response to the data access request complies with the requirements of the GDPR.
5.2.2 Data subjects have the right to complain to OVT related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

6.0 Consent

6.1 OVT understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed, and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. The data subject can withdraw their consent at any time.

6.2 OVT understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be a valid basis for processing.

6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. OVT must be able to demonstrate that consent was obtained for the processing operation.

6.4 For sensitive data, explicit written consent (Consent Procedure) of data subjects must be obtained unless an alternative legitimate basis for processing exists.

6.5 In most instances, consent to process personal and sensitive data is obtained routinely by OVT using standard consent documents e.g., when a new client ticks to indicate their consent to relevant processing when they sign up with us, or during induction for participants on programmes or employee recruitment.

7.0 Security of data

7.1 All Employees/Staff are responsible for ensuring that any personal data that OVT holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by OVT to receive that information and has entered into a confidentiality agreement and or contract detailing said authorisation. (Information Security Policy)

7.2 All personal data will only be accessible to those who need to use it, and access may only be granted in line with the IT Access Control Policy. All personal data will be treated with the highest security and must be kept:

- If hard copy, in a lockable room with controlled access; and/or
- If hard copy, in a locked drawer or filing cabinet; and/or
- If electronic, password protected in line with the requirements in the IT Access Control Policy; and/or
- If electronic, stored on (removable) computer media that is encrypted in line with Secure Disposal of Data inc. Hardware Procedure.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of OVT. All Employees/Staff must abide by the IT Access Control and Information Security Policy prior to being given access to organisational information of any sort.

7.4 Hard-copy records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as hard-copy records are no longer required for day-to-day client support, they must be removed from secure archiving in line with Data Retention Procedure.

7.5 Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Hard-copy records that have reached their retention date are to be shredded and disposed of as 'confidential waste' through an approved process. Hard drives of redundant PCs are to be removed and immediately destroyed as required by Secure Disposal of Data inc Hardware Procedure before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data. Staff must be specifically authorised to process data off-site.

7.7 Should data which is processed for an on behalf of customers require deletion or disposal either from hardware and or in electronic format, will be through (formal written) request from the customer and approval by the department Executive prior to deletion or disposal.

8.0 Disclosure of data

8.1 OVT will ensure that personal data is not disclosed to unauthorised third parties, which include family members, friends, government bodies and, in certain circumstances, even the police (unless OVT is lawfully required to do so). All Employees/Staff must exercise caution when asked to disclose personal data held on another individual to a third party.

It is important that Employees/Staff bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of OVT 's business and if in doubt seek clarification from line managers and or the Compliance Manager.

8.2 All requests to provide data for any reason must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the department executive and or HR and or the Compliance Manager, as a minimum a combination of two departments.

9.0 Retention and disposal of data

9.1 OVT will not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 OVT may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the Data Retention Procedure along with the criteria used to determine this period, including any statutory obligations OVT have to retain the data.

9.4 OVT 's data retention and data disposal procedures will apply in all cases.

9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the 'rights and freedoms' of data subjects. Any disposal of data will be done in accordance with the Secure Disposal of Data inc. Hardware Procedure.

10. Data transfers

10.1 The GDPR requires certain additional considerations to be made and appropriate safeguards to be put in place before personal data is transferred overseas (i.e. outside the UK or the EU, as appropriate). OVT complies fully with these safeguards and where it transfers data overseas, it shall ensure that it:

10.1.1 is transferring Personal Data to a country (or a territory or sector within a country) which at the time of transfer is formally recognised by the UK (or the European Commission in the case of a transfer from an EU Member State) as providing an adequate level of data protection; or

10.1.2. OVT has put in place appropriate safeguards itself to protect such personal data and ensure that the relevant data subjects have enforceable subject access rights and effective legal remedies as required by the applicable territory's laws, such as a lawful and appropriate contract with the data importer (commonly known as 'standard contractual clauses') along with an appropriate risk assessment (commonly known as a transfer adequacy assessment). Should OVT utilise the SCCs we will make our staff/employees, customers, third parties and stakeholders aware of this.

10.1.3 Should OVT need to transfer personal data from the UK to countries not covered by the UK's adequacy regulations, we will provide appropriate safeguards, such as an International Data Transfer Agreement (IDTA) or the International Data Transfer Addendum (UK Addendum) introduced by the UK Information Commissioner (ICO) in March 2023. These IDTA are essentially the UK version of the new EU Standard Contractual Clauses (SCCs) detailed in 10.1.2 that take into account the GDPR and the Schrems II case.

10.2 Where an adequacy decision or SCCs are not appropriate, OVT will only transfer personal data overseas where:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise, or defence of legal claims.
- The transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11.0 Information asset register/data inventory

11.1 OVT has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance projects. OVT 's data inventory and data flows determine;

- Business processes that use personal data;
- Sources of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- And maintain the inventory of data categories of personal data processed; And document the purpose(s) for which each category of personal data is used; Recipients, and potential recipients, of the personal data;
- The role of OVT throughout the data flow;
- Key systems and repositories;

- Any data transfers; for personal data flows, OVT will consider and record whether there are any transfers of personal data in terms of crossing international borders, different regulations and laws will be considered should data transfers be required.
- All retention and disposal requirements.

11.2 OVT ensures awareness of any risks associated with the processing of types of personal data.

11.2.1 OVT assesses the level of risk to individuals associated with the processing of their personal data through;

- Data protection impact assessments (DPIAs), which are supported and detailed within the system;
- Data Protection Impact Assessment Procedure;
- Project Specific Risk Assessments;

Which are carried out in relation to the processing of personal data by OVT, and in relation to processing undertaken by other organisations on behalf of OVT.

11.2.2 OVT shall either manage and or mitigate any risks identified by the risk assessment to reduce the likelihood of a nonconformity with this policy and its associated systems.

11.2.3 Where a type of processing, using new technologies and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, and as such OVT shall, before the processing, carry out a DPIA on the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, because of a DPIA, OVT is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not OVT may proceed must be escalated for review to the Chief Operating Officer and or Senior VP for Compliance and Finance and with regard to the ONVU Learning product set, the VP Commercial ONVU Learning.

11.2.5 The Compliance Manager shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the relevant supervisory authority.

11.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to OVT ’s documented risk acceptance criteria and the requirements of the GDPR.

12.0 Review

12.1 This Policy will be reviewed annually or sooner should the need arise through legislative changes and or a breach or changes in company structure or customer requirements or;

12.1.2 where an update to another business entity and or policy requires a change to this policy.

Revised on	Version	Description	Approver
22.11.2021	Issue V1	Full issue	Compliance
08.12.2022	Issue V2	Full revision as to appropriateness, changes to 2.6, references to associated internal policy and nomenclature throughout. Inc insertion of review section table.	Compliance
24.04.2023	Issue	Updated to meet the naming convention as per the document control procedure 3.4.7 naming of Data Training Policy; 4.2 addition of link to employee privacy notice; 4.5.4 doc procedure not policy; consent 6.4; 11.2.1 data protection impact assessment; Footer removed as externally required doc	Compliance Manager
13.09.2023	Issue	Various amends as per MIS and UAE Considerations and updates to links throughout	Compliance
15.09.2023	Draft	Sent for review	Compliance
19.09.2023	Draft	Appendix of 3rd parties added	Compliance
26.09.2023	Issue	Ready for review with VP OVL	Compliance
27.09.2023	Issue	Amends addressed, OVL PN removed	Compliance

Appendix 1

Table of Third Parties

Data processors are third parties who provide certain parts of our services for us. We have contracts in place with them and they cannot do anything with your personal information unless we have instructed them to do so. Our current data processors are listed below.

Data Processor	Purpose	Privacy Notice
AWS	Cloud services	Amazon Web Services
FedEx	Courier service	FedEx
Microsoft	All systems	Microsoft
NSPCC	Safeguarding training	NSPCC
Zendesk	Customer service platform	ZenDesk
PandaDoc	Document automation software	PandaDoc
HubSpot	Customer Relationship Management Software.	HubSpot
ChargeBee	Subscription Platform	ChargeBee
Quick Books	Accounting	QuickBooks
Wonde	Management Integration System	Wonde
SAP	Financial Management	SAP
UPS	Courier Services	UPS