Avado Data Protection Policy

1 About this policy

Individuals have rights under national or international data protection laws and regulations regarding how their personal information is being used by companies.

As an internationally operating group venture, Avado is governed by a variety of national and international data protection laws. This policy is here to guide and inform about our regulatory requirements under the UK and EU General Data Protection Act (GDPR). Information regarding national laws can be found in the relevant addendums to this Policy at the bottom of the policy.

2 Status of the policy

This policy sets out the Company's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information. The Data Protection Officer (DPO) is responsible for the overall implementation and adherence to the GDPR. The Avado Compliance Team are your first point of contact regarding any questions you may have when it comes to data protection.

If a member of staff considers that this policy has not been followed in respect of their personal data, or the personal data of others (i.e. customers), they should raise the matter with the DPO, the Avado Compliance Team or the People Experience Team (HR).

3 Scope

The policy relates to all the Avado staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Avado)* and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

4 Definition of data protection terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Avado means the Avado trading subsidiaries, including but not limited to Avado Learning Limited, Avado Asia Pacific PTE LTD, Avado Hong Kong PTE LTD, Avado Apprenticeships Limited FastFutures Limited

Data is any information which is stored or otherwise processed in any format by Avado staff or automated systems

Data subject means a natural person;

Natural Person means a human being, as opposed to a legal person

Legal Person means a legal entity or organisation

General Data Protection Act *or* ***GDPR*** means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, more commonly known as the General Data Protection Regulation

Personal data has the same meaning as defined under the GDPR, 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

Encryption means the process of converting information or data into a code to prevent unauthorized access.

Pseudonymisation has the same meaning as defined under Article 4 of the GDPR, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Special categories of personal data (otherwise known as sensitive personal data) means information regarding race, ethnic origins, pollical opinions, religion, philosophical beliefs, trade union membership, genetic data for the purpose of uniquely identifying a natural person, biometric data for the purpose of uniquely identifying a natural person, health data, data concerning a natural person's sex life, sexual orientation.

Data controller (or **controller**) has the same meaning as defined under Article 4 of the GDPR, a 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;

Data processor (or **processor**) has the same meaning as defined under Article 4 of the GDPR, a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data Protection Officer (DPO) means the named person within the business which is overall responsible for the oversight and implementation of GDPR and acts as a point of contact for the data subjects.

Processing has the same meaning as defined under Article 4 of the GDPR, any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It's the responsibility of everyone in the organisation to respond to a security incident and we have 72 hours to investigate, assess and, where relevant report the incident.

European Economic Area (EEA) means Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

5 Data protection principles

Anyone processing personal data must comply with the six enforceable principles of good practice. These provide that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

6 General Staff Guidelines

- Data should only be shared with individuals who strictly require it in line with their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers or data owners
- Employees should keep all data secure by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they must never be shared
- Personal data should not be disclosed to unauthorised people, disregarding of whether it is shared internally or externally
- Data should be regularly review and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should seek guidance from the Avado Compliance Team if they are unsure about any aspect of data protection or their responsibilities for the protection of data and best practises

7 Data Storage

When data is stored on paper, it should be kept in a secure place where only authorised people can see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet;
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for example on a printer;
- Data printouts should be shredded or disposed of using the confidential waste;

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media, it must be encrypted and stored securely
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud storage service
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Company's standard backup procedures
  Data should never be saved directly to un-encrypted laptops or other mobile devices like tablets or smart phones
  All servers and computers containing data should be protected by approved security software and a firewall

7.1 Fair and lawful processing

The GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights and freedoms of the data subject. The data subject must be told who the data controller is (in this case the Company), who the data controller's representative is (in this case the DPO or representative), the purpose for which the data is to be processed and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, one of the regulatory exceptions for processing of special categories of data must be met in order to process the data in a lawful and compliant manner. In most cases the data subject's explicit consent to the processing of such data will be required.

The following is a non-exhaustive list of the type of data we may hold on file but more can be found in the Avado Data Retention Policy:

- Details supplied on application forms and any accompanying CV
- Interview notes
- References received
- Job description
- Contracts
- Performance review forms and associated documents
- Copies of any direct correspondence with employees
- Disciplinary records
- All file notes relating to management of employees
- Medical certificates, self-certificates and fit notes
- Medical questionnaires
- Leaner / student records
- Other information covering periods of absence, training records and any other material as is considered appropriate by the Data Controller

7.2 Processing for limited purposes

Personal data may only be processed for the specific purposes for which the data was collected by the data. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must normally be informed of the new purpose before any processing occurs.

7.3 Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

7.4 Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed

7.5 Timely processing

Personal data should not be kept longer than is necessary for the purpose it was collected. This means that data should be destroyed or erased from the Company's systems when it is no longer required. Guidance on data retention can be found in the Avado Data Retention Policy.

If data has been collected for a specific purpose and such purpose may change, please consult with the Avado Compliance Team about further steps.

7.6 Processing in line with data subjects' rights

Data must be processed in line with the data subjects' rights under the regulations:

- Right to access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subject to decision making based solely on automated processing, including profiling

8 Data security

The Company must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The regulations require us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (short CIA) of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Company's central computer system instead of individual PCs.

For information how Avado is protecting data, please consult the following policies respectively:

- Avado Access Control Policy
- Avado Backup Policy
- Avado Clear Desk Policy
- Avado Cryptographic Controls Policy
- Avado Information Exchange Policy
- Avado Information Sensitivity Policy
- Avado Information Security Policy
- Avado Laptop Policy
- Avado Malicious Software Protection Policy
- Avado Network Systems Monitoring Policy
- Avado Password Policy
- Avado Remote Access and Mobile Computing Policy
- Avado Security Incident Reporting Policy
- Avado USB Memory Sticks Usage Policy

9 Dealing with subject access requests

Subject access requests are a request for information or execution of the rights of the data subjects and come through in any format. For more information, please consult the Avado Subject Access Request Policy and Procedures.

10 Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked
- Refer to their manager or the Avado Compliance Team for assistance in difficult situations. No-one should be pressured into disclosing personal information.

11 Monitoring and review of the policy

This policy is reviewed from time to time by the Avado Compliance or Information Security Team. The Company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

National Appendix

Data and personal data will be processed in line with national data protection laws.

12 Document Control

DOCUMENT NAME	VERSION	MASTER COPY LOCATION
Avado Data Protection Policy	1.6	Avado Compliance SharePoint

Unless stated within the body of this document, the owner is responsible for maintaining document control and facilitating compliance; as well as the management of review, updates and changes.

OWNER	ROLE / ORGANISATION	CONTACT
Dougie Reid	**DPO**	**dataprotection@avadolearning.com**
AUTHOR	**ROLE / ORGANISATION**	**CONTACT**
Sascha Peter	Group Information Security Officer	Sascha.peter@avadolearning.com

12.1 Revision History

Version	Date	Amended By	Summary of changes
1.1	2018-10-02	Sascha Peter	Update to GDPR / DPA 2018 + Formatting
1.2	2018-10-23	Sascha Peter	Update with regards to feedback from internal + DPO
1.3	2019-04-11	Sascha Peter	Update definitions to put in line with others
1.4	2020-01-03	Sascha Peter	Annual review and update terminology and minor content changes
1.5	2021-03-17	Sascha Peter	Content review and update with branding.
1.6	2023-6-7	Keith Harvey	Legal Entity Update

12.2 Document Reviews

This document has been reviewed for QC purposes by the following, in addition to those on the 'approvers' list.

Version	Date	Name	Title / Role
1.0	2018-10-02	Sascha Peter	Information Security Analyst
1.1	2018-10-09	Dougie Reid	DPO
1.2	2019-04-11	Sascha Peter	Information Security Analyst
1.3	2020-01-03	Sascha Peter	Group Information Security Officer
1.4	2021-03-17	Sascha Peter	Group Information Security Officer
1.5	2021-03-18	Keith Harvey	Head of Risk and Compliance

12.3 Approvals

This document requires the following approvals for implementation and / or for any change in content.

Version	Date	Name	Title / Role	Approval Status (Pending/Approved)
1.2	2018-10-02	Keith Harvey	Head of Student Services and Compliance	Approved
1.2	2018-10-02	Dougie Reid	DPO	Approved
1.3	2019-04-11	Keith Harvey	Group Risk and Compliance Manager	Approved
1.3	2019-04-11	Dougie Reid	DPO	Approved
1.4	2020-01-03	Keith Harvey	Group Risk and Compliance Manager	Approved
1.4	2020-01-03	Dougie Reid	DPO	Approved
1.5	2021-03-16	Dougie Reid	DPO	Approved
1.5	2021-03-18	Keith Harvey	Head of Group Compliance	Approved
1.6	2023-6-7	Keith Harvey	Director of Compliance, Funding and Audit	Approved