Data Protection Policy at Universal AI University

Date	Revision No	Issue No	Prepared By	Approved By
21.05.2015	1	1		Executive Council
07.05.2022	1	2	Dr. Tapas	

Data Protection Policy at Universal AI University

Introduction

Universal AI University takes the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. This policy sets out how the university manages those responsibilities effectively. Universal AI University obtains, uses, stores and otherwise processes personal data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts, collectively referred to in this policy as data subjects. Whileprocessing personal data, the university is obliged to fulfil both individuals' reasonable expectations of privacy by complying with GDPR and also relevant data protection legislation (data protection law). This policy therefore seeks to ensure that we:

1. How personal data must be processed and vis-a-vis university's expectations for all those who process personal data on its behalf.
2. Comply with the data protection law and with good industry practice.
3. Protect the University's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
4. Protect the university from risks of personal data breaches and other breaches of data protectionlaw.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored and regardless of the data subject. All staff and others processing personal data on the university's behalf must read it. A failure to comply with this policy may result in disciplinary action. All Heads of Programs and Directors are responsible for ensuring that all university staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance. The university's Data Protection Officer (DPO) is de-facto IT Head.

Personal data protection principles

The university is responsible for, and must be able to demonstrate compliance with, the dataprotection principles listed below: Those principles require personal data to be:

1. Process lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency). Detail on how to achieve this can be found in Appendix 1.

2. Collected only for specified, explicit and legitimate purposes and not in a manner incompatible with those illegitimate purposes (Purpose limitation). Detail on how to achieve this can be found in Appendix 2
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation). Detail on how to achieve this can be found in Appendix 2.
4. Accurate and wherever necessary keep up to date (Accuracy). Detail on how to achieve this can be found in Appendix 2.
5. It should be stored such that it meets requirement of minimum record keeping duration, data subjects for longer than is necessary for specific purpose, please refer Appendix 2.
6. Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality). Detail on how to achieve this can be found in Appendix 2.

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. Where the legal basis of our processing is Consent, to withdraw that Consent at any time;

2. Asking for access to the personal data that we hold (see below);

3. Prevent use of the personal data for direct marketing purposes

4. Objecting to our processing of personal data in limited circumstances

5. Asking us to erase personal data without delay:

a. If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

b. If the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;

c. If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

d. If the data subject has objected to our processing for direct marketing purposes;

e. If the processing is unlawful.

f. Ask us to rectify inaccurate data or to complete incomplete data;

6. To restrict processing in specific circumstances e.g., where there is a complaint about accuracy;
7. The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the University; itis based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
8. To prevent processing that is likely to cause damage or distress to the data subject or anyone else;
9. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
10. To make a complaint to the law; and in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g., another University to which a student is transferring) in astructured, commonly used and machine-readable format.

DPO (Data Protection Officer) verifies the identity of an individual requesting data under any of the rights listed

Accountability

The University must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The University is responsible for, and must be able to demonstrate compliance with, the data protection principles. The University appliesadequate resources and controls to ensure and to document compliance including:

1. Appointing a suitably qualified DPO;
2. Implementing Privacy by Design when processing personal data
3. Integrating data protection into policies and procedures, in the way personal data is handled and produced require documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
4. Training staff on compliance with Data Protection Law and keeping a record accordingly; and
5. Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance

Responsibilities

University responsibilities

1. As the Data Controller, the University is responsible for establishing policies and procedures inorder to comply with data protection law.
2. Data Protection Officer responsibilities The DPO is responsible for:

   (a) Advising the University and its staff of its obligations under GDP Law

(b) Monitoring compliance with this Regulation and other relevant data protection law, the University's policies with respect to this and monitoring training and audit activities relate to GDP Policycompliance

(c) To provide advice were requested on data protection impact assessments

(d)To cooperate with and act as the contact point for the Stakeholders

(e) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3. Staff responsibilities Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) all personal data is kept securely;

(b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

(c) personal data is kept in accordance with the University's retention schedule;

(d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO

(e) any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the team in resolving breaches;

(f) where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer.

Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from Data Protection Officer.

4. Third-Party Data Processors Where external companies are used to process personal data on behalf of the University, responsibility for the security and appropriate use of that data remains with the University. Where a third-party data processor is used:

a. A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
b. Reasonable steps must be taken that such security measures are in place;
c. A written contract establishing what personal data will be processed and for what purpose must be set out;
d. A data processing agreement, available from DPO, must be signed by both parties. For further guidance about the use of third-party data processors please contact the DPO

5. Contractors, Short-Term and Voluntary Staff;

The University is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

a. Any personal data collected or processed in the course of work undertaken for the University is kept securely and confidentially;
b. All personal data is returned to the University on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed andthe University receives notification in this regard from the contractor or short term / voluntary member of staff;
c. The University receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
d. Any personal data made available by the University, or collected in the course of the work,is neither stored nor processed outside the country unless written consent to do so hasbeen received from the University;
e. All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

6. Student responsibilities

Students are responsible for

a. Familiarising themselves with the Privacy Notice provided when they register with the University;
b. Ensuring that their personal data provided to the University is accurate and up to date.

7. Data subject Access Requests

Data subjects have the right to receive copy of their personal data which is held by the University. In addition, an individual is entitled to receive further information about the University's processing oftheir personal data as follows:

1. The purposes
2. The categories of personal data being processed
3. Recipients/categories of recipient
4. Retention periods
5. Information about their rights
6. The right to complain to the Law,
7. Details of the relevant safeguards where personal data is transferred outside the country
8. Any third-party source of the personal data

Reporting a personal data breach

The GDP Policy requires reporting to any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g., encryption). or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action. Procedures are in place to deal with any suspected personal data breach and will notify data subjects or the Law where we are legally required to do so.

Record Keeping

At UNIVERSAL AI UNIVERSITY the Policy is to keep full set of data uncorrupted and fully protected during the entire period.The University maintains accurate corporate records reflecting processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing. These records include, at a minimum, the name and contact details of the University as DataController and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of thesecurity measures in place. Records of personal data breaches must also be kept, setting out:

1. The facts surrounding the breach

2. Its effects; and
3. The remedial action taken

Training and Audit

The University ensures that all University staff undergo adequate training to enable them to comply with data protection law. It also regularly tests systems and processes to assess compliance.

Data privacy by design and default

Privacy-by-design – is the theme, while processing personal data. By implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, itensures compliance with data-protection principles. It ensures by default only personal data which isnecessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the 7 processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons.

Direct Marketing

Universal AI University is subject to certain rules and privacy laws when marketing to our applicants, students,alumni and any other potential user of our services. For example, a data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limitedexception for existing customers (e.g., current students) known as "soft opt in" allows organizations to send marketing texts or emails if they have obtained contact details in the course of a sale to thatperson, they are marketing similar services (e.g., a post-graduate course or a professional qualification), and they gave the person an opportunity to opt out of marketing when first collectingthe details and in every subsequent message. The right to object to direct marketing is explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be promptly honored. If a data subject opts out at any time, their details are suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data

In the absence of Consent, a legal obligation or other legal basis of processing, personal data is not generally disclosed to third parties unrelated to the University (e.g., members of the public,private property owners).

Changes to this policy

Universal AI University reserves the right to change this policy at any time without notice so please checkregularly to obtain the latest copy. This policy was approved on 21 May 2015 by the Executive Council.

Appendix 1

Principle 1 of GDP Policy – Processing personal data lawfully, fairly and transparently

1. **Lawfulness and fairness**

Personal data can be processed fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, the

University may only process personal data if the processing in question is based on one (or more) of the legal bases set out below. Section 4.3 below deals with justifying the processing of sensitive personaldata. Including special category data. The legal bases for processing non-sensitive personal data are as follows:

1. The data subject has given his or her Consent
2. The processing is necessary for the performance of a contract with the data subject

(e.g., monitoring academic performance in order to provide the relevant qualification for which the student has enrolled)

3. To meet our legal compliance obligations
4. To protect the data subject's vital interests (i.e., matters of life or death)
5. To pursue our legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that the University is pursuing when processing personal data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private functions e.g., marketing, fundraising and not for public functions. The Universityidentifies the legal basis that is being relied on for each processing activity, which will be included inthe Privacy Notice provided to data subjects.

1. Consent

UNIVERSAL AI UNIVERSITY only obtains a data subject's Consent if there is no other legal basis for the processing. Consent requires genuine choice and genuine control. A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Data subjects are able to withdraw Consent to processing easily at any time. Withdrawalof Consent is promptly honoured Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences is treated in the same way to special category data.

Processing of sensitive personal data

The processing of sensitive personal data by the University must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

1. The data subject has given explicit Consent (requiring a clear statement, not merely an action)
2. The processing is necessary for complying with employment law;

3. The processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving Consent;
4. The processing relates to personal data which are manifestly made public by the data subject;
5. The processing is necessary for the establishment, exercise or defence of legal claims;
6. The processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject)
7. The processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality
8. The processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;
9. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if it is subject to certain safeguards (i.e., pseudonymisation or anonymisation where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

Examples of sensitive personal data processed by the University will include:

i. Details of relevant unspent convictions for the purposes of assessing eligibility to enrol on the University's academic programmes
ii. Details of relevant unspent convictions for the purposes of recruiting relevant staff
iii. Checks conducted by the Disclosure and Barring Service for the purposes of assessing eligibility of staff or students to engage in work with children and vulnerable adults, as permitted by legislation relating to the rehabilitation of offenders or for determining fitness to practise relevant professions
iv. Unspent convictions or allegations of sexual misconduct for staff and student disciplinary purposes
v. Health data for the purposes for assessing eligibility to undertake relevant professional programmes, assessing fitness to study or to engage in university activities or for assessing fitness to work/occupational health
vi. Details of disability for the purposes of assessing and implementing reasonable adjustments to the University's policies, criteria or practices

vii. Details of racial/ethnic origin, sexual orientation, religion/belief for the purposes of equality monitoring Processing sensitive personal data represents a greater intrusion into individual privacy than when processing non-sensitive personal data. University takes special care when processing sensitive personal data and ensures compliance with the dataprotection principles (as set out in the main body of this policy) and withthis policy, in particular in ensuring the security of the sensitive personal data.

2. Transparency (notifying data subjects)

Under the GDP Policy the University is required to provide detailed, specific information to datasubjects depending on whether the information was collected directly from data subjects orfrom elsewhere. That information is provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject easily understands what happens to their personal data. Whenever wecollect personal data directly from data subjects, for example for the recruitment and employment of staff and for the recruitment and enrolment of students, at the time of collection UNIVERSAL AI UNIVERSITY provides the data subject with all the prescribed information which includes:

a) University's details
b) Contact details of DPO
c) Purposes of processing
d) Legal basis of processing
e) Where the legal basis is legitimate interest, identify the particular interests (e.g.,marketing, fundraising)
f) Where the legal basis is Consent, the right to withdraw
g) Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision

Appendix 2

Principle 1 of GDP Policy - Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes.It must not be further processed in any manner incompatible with those purposes. University does not therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing

is not based on the data subject's Consent or on a lawful exemption from data- protection law requirements, University assesses whether a purpose is incompatible bytaking into account factors such as:

1. the link between the original purpose/s for which the personal data was collected and the intended further processing
2. the context in which the personal data has been collected – in particular the University-data subject relationship. You should ask yourself if the data subject would reasonably anticipate the further processing of his/her personal data
3. the nature of the personal data in particular whether it involves special categories of personal data (i.e., sensitive) or personal datarelating to criminal offences/convictions
4. the consequences of the intended further processing for the data subjects
5. the existence of any appropriate safeguards e.g., encryption or pseudonymisation.

Principle 2 of the GDP Policy

Data minimisation Personal data must be adequate, relevant and limited to what isnecessary in relation to the purposes for which it is processed. The University does not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed. University ensures that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the University's data retention policy and schedule.

Principle 3 of the GDP Policy

Accuracy Personal data must be accurate and, where necessary, kept up to date. UNIVERSAL AI UNIVERSITY ensures that personal data is recorded in the correct files. Where a data subjecthas required his/her personal data to be rectified or erased, DPO informs recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 4 of the GDP Policy

Security, Integrity and Confidentiality the university is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e., that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. Each employee is also responsible for protecting the personal data that you process in the course of their duties. They must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. They must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure. University also complies with all procedures andtechnologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. All employees must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data P