HEA | AN tÚDARÁS um ARD-OIDEACHAS HIGHER EDUCATION AUTHORITY

Data Protection Policy

THE HEA DATA PROTECTION POLICY

Contents

Version Control

1 – Prepared by Data Protection Unit with Mazars assistance July 2019

2- Updated by DPO February 2021

1 INTRODUCTION

The HEA and the Irish Research Council[1] are committed to ensuring the lawful, fair and transparent processing of Data Subjects personal data through the use of appropriate technical and organisational measures. The HEA will take all reasonable steps to secure and protect Data Subjects personal data while complying with Data Protection Law.

The purpose of the EU General Data Protection Regulation 2016/679 (the "GDPR") and other related regulations and delegated national legislation (such as the Data Protection Acts 1998, 2003 and 2018) (together "Data Protection Law") are to protect the privacy of individuals whose personal data is processed. Personal data means any information relating to an identified or identifiable natural person (the data subject). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data or online identifier.

2 SCOPE AND PURPOSE

This policy applies to all personal data collected, processed and stored by the HEA in respect of all data subjects (i.e. applicants, students, staff and service providers) Personal data may be contained in records of many forms throughout the HEA including hardcopy data, electronic data, information held on portable devices, and CCTV footage.

The purpose of this Data Protection Policy is to enable the HEA to:

- Ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
- Ensure that the HEA fully respects the rights and privacy of all customers, staff and other data subjects whose data is processed by the HEA.
- Protect the organisation, customers, staff and other data subjects from the consequences of a data breach.

This policy should be read in conjunction with other relevant HEA policies and procedures.

3 POLICY RESPONSIBILITY

The Board of the HEA are committed to compliance with all relevant EU and Irish laws in respect of personal data, and to the protection of the rights and freedoms of data subjects whose information the HEA collects and processes.

The Senior Management Team are responsible for ensuring that this policy is implemented in their respective Sections and Business Units. Managers at all levels are responsible for being able to demonstrate that this policy is being implemented.

[1] The Irish Research Council operates under the aegis of the Higher Education Authority, this policy applies to data held by the Council.

All staff and contractors located in the HEA have a responsibility to comply with the HEA's Data Protection Policy.

The Data Protection Policy shall be maintained by the Data Protection Officer (DPO). It shall be the responsibility of the DPO to ensure that this policy is kept up-to-date and meets the requirements of the HEA and relevant legislation.

4 WHAT IS DATA PROTECTION?

The purpose of "Data Protection Law" is to protect the privacy of individuals whose personal data is being processed.

Processing data includes the collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission or dissemination and restriction, erasure or destruction. It relates to both automated data (i.e. computer held records) and manual data.

Personal data is information relating to a living individual who can be identified from the data itself or in conjunction with other information held. This may include name, address, academic information, contact details etc.

Special Category Data is 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 (GDPR Art. 9 (1)). Special Category Data can only be processed under strict conditions.

Criminal Data is information relating to criminal convictions and offences. Criminal Data can only be processed in accordance with EU or Irish law and subject to appropriate safeguards put in place for the purposes of processing this type of data.

Data Subject is an identifiable natural person 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. Examples of data subjects which may be relevant to the HEA include Employees, students, applicants, assessors and so on.

5 DATA PROTECTION PRINCIPLES

There are a number of principles under the Data Protection Law which must be satisfied when processing personal data.

5.1 ACCOUNTABILITY

As a Data Controller, the HEA shall be responsible for, and must be able to demonstrate compliance with Data Protection Law. This means that the HEA must comply with and demonstrate that the key principles of Data Protection are met when it comes to all personal data for which the HEA is

responsible. Where the HEA is a Data Processor it shall maintain its commitment to compliance with Data Protection Laws and shall assist Data Controllers, where necessary, in demonstrating their compliance.

5.2 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data can only be processed lawfully, fairly and in a transparent manner. This means that the HEA must inform Data Subjects about the kind of processing their personal data will be subjected to (transparency), that the processing must match the description given to the Data Subjects (fairness) and that the processing must be for one of the lawful basis specified to the Data Subjects at time of collection (lawfulness). Lawful basis includes; consent, contract, legal obligation, vital interests, public interest, and, legitimate interest. The HEA is governed by the Higher Education Authority Act, 1971 and most of our data processing is done under this law.

5.3 PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. This means that the HEA should specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose. Further processing for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes shall not be incompatible with the specified purpose. Where the HEA seeks to further process data for purposes other than those for which the data was originally collected, it shall carry out an assessment to see whether this is lawful and compatible with the original purpose.

5.4 DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that the HEA should not retain any personal data beyond what is strictly required to achieve the purposes for which the personal data was collected.

5.5 ACCURACY

The HEA will take all possible steps to ensure that all personal data held is accurate and up to date and that all data collection procedures will be designed to ensure that reasonable steps are taken to update personal data where new data has been provided.

5.6 STORAGE LIMITATION

Personal data shall be kept for no longer than is necessary for the purposes for which the personal data is collected and shall be kept in line with the HEA Retention Policy. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes.

5.7 SECURITY/INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The HEA will use appropriate technical and organisational measures to protect the integrity and confidentiality of personal data. This includes physical security measures such as swipe cards to gain access to the office, and operating a clean desk policy.

6 DATA SUBJECTS' RIGHTS

Data Subjects have a number of rights under the GDPR. These rights can be applied by making the appropriate request to the HEA using the forms included below. In processing a Data Subject request, the HEA will:

- Check whether the organisation holds personal data on the Data Subject
- Check the validity of the request by confirming the identity of the person making the access request
- Decide if the request is excessive or manifestly unfounded or if the request will be refused
- Determine if a charge may be applied if the request is deemed to be unjustified or excessive
- Determine if additional information or clarification is required from the Data Subject in order to process the request
- Determine if the request can be answered within 30 days or if an extension is required
- Determine if the request complies with the specific requirements of the Data Protection Law
- Determine if any exemptions are to be applied to the request

Where the HEA is legally permitted to do so, the HEA may decline a Data Subject's request. Such a refusal will be explained to the Data Subject in writing. Please note that Data Subject rights are not absolute. Exceptions or limitations relating to certain of the rights conferred by the GDPR are noted below in the relevant section. There is a separate procedure document on how to process Subject Access Requests available on the staff Intranet.

Data Subjects have the following rights under the GDPR/Data Protection Act 2018:

6.1 RIGHT OF ACCESS

Under Article 15 GDPR, Data Subjects have a right to request access to a copy of their personal data. In addition, other information relating to the processing; sharing and retention of their personal data must also be provided to the Data Subject when processing a Subject Access Request.

6.2 RIGHT TO RECTIFICATION

Under Article 16 GDPR, Data Subjects have a right to have their personal data rectified if it is inaccurate or incomplete. If this personal data has been shared with third parties, the HEA will notify such third parties about the rectification request from the Data Subject unless this is impossible or involves disproportionate effort. Where it is deemed reasonable for the HEA not to comply with a Data Subject request for rectification, this decision will be explained to the Data Subject in writing.

6.3 RIGHT TO ERASURE

Under Article 17, GDPR, Data Subjects have a right to erasure of their personal data where one of the following grounds apply:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- The Data Subject withdraws consent and there is no other legal basis for the processing
- The Data Subject objects to the processing pursuant to article 21(1)
- The personal data have been unlawfully processed
- The personal data have to be erased for compliance with a legal obligation
- The personal data have been collected in relation to the offer of information society services of a child.

A request for Erasure of personal data can be refused where processing is necessary:

- For exercising the right to freedom of expression and information
- For compliance with legal obligation or for the performance of a public interest task or exercise of official authority
- For Public health reasons
- For archiving interests in the public interest, scientific, historical research or statistical purposes
- For the exercise or defence of legal claims

6.4 RIGHT TO RESTRICTION OF PROCESSING

Under Article 18 GDPR, Data Subjects have a right to Restrict the Processing of their personal data where one of the following grounds apply:

- Where the Data Subject contests the accuracy of their personal data (processing should be restricted for a period enabling the HEA to verify the Data's accuracy)
- Where the processing is unlawful and the Data Subject opposes erasure and requests restriction instead
- Where the controller no longer needs the personal data but the Data Subject requires the HEA to continue to process the personal data to exercise or defend a legal claim
- Where the Data Subject has objected to the processing; processing should be restricted pending verification of whether the legitimate interests of the controller override those of the Data Subject. Article 18(1).

When a Data Subject exercises their right to restrict processing, the HEA will only continue to process the personal data if:

- The Data subject consents
- The processing is necessary for the exercise or defence of legal claims
- The processing is necessary for the protection of the rights of other individuals or legal persons
- The processing is necessary for Public Interest reasons under EU/Member State law

The HEA will inform the Data Subject before the processing restriction is lifted/enforced.

6.5 RIGHT TO DATA PORTABILITY

Under Article 20 GDPR, Data Subjects have a right to receive the personal data they have provided to the HEA in a structured, commonly used and machine readable format. Data Subjects have the right to have their personal data transmitted to another controller. The right applies to personal data a Data Subject has provided to the HEA and to personal data generated by an individual's activity but does not extend to data generated by the HEA. The right to Data Portability only applies if:

- The processing is based on the Data Subject's consent or for the performance of a contract and
- The processing is carried out by automated means

The right to Data Portability will not apply to processing necessary for the performance of a task carried out in the Public Interest, or in the exercise of official authority vested in the HEA. In addition, the right to Data Portability must not adversely affect the rights and freedoms of others. Data Portability does not automatically trigger the erasure of the Data Subjects personal data from the HEA systems/processes and does not affect the original retention period applying to the personal data.

Please note that the HEA may keep a record of a Data Subject's communications to resolve any issues which a Data Subject raises.

6.6 RIGHT TO OBJECT

Under Article 21 GDPR, Data Subjects have a right to object to the processing of their personal data on the following grounds:

- Direct marketing; where personal data are processed for direct marketing purposes, the Data Subject has the right to object at any time to such processing; there are no grounds to refuse to comply with such a request. When a Data Subject objects to processing for direct marketing purposes, the personal data can no longer be processed for that purpose.
- Processing based on public interest or legitimate interest grounds, including profiling.

- Processing for scientific, historical research or statistical purposes (unless the processing is necessary for the performance of a public interest).

When a Data Subject objects to the processing of their personal data, the HEA will stop processing the personal data unless the HEA can demonstrate that there are compelling legitimate grounds for the processing which override the rights of the Data Subject; the processing is necessary for the exercise or defence of legal claims or the personal data is processed for scientific, historical research or statistical purposes, the processing of which is necessary for the performance of a public interest/task.

6.7 RIGHT TO OBJECT TO AUTOMATED DECISION-MAKING, INCLUDING PROFILING

Under Article 22 GDPR, Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effect concerning the Data Subject.

Where a decision based solely on automated processing, including profiling, occurs on the basis that it is necessary for the performance of a contract or with the explicit consent of the Data Subject; the Data Subject will be given "at least the right" to express their point of view and to contest the decision. Article 22(3).

Automated Decision Making involving sensitive data is only allowed where the Data Subject has given their explicit consent, or it is necessary for the public interest. Article 22(4).

The HEA will inform Data Subjects at the time the personal data is collected of the existence of Automated Decision Making, including profiling.

The HEA may not comply with the objection if the processing is necessary for the performance of a contract; the processing is authorised by EU or Member State law or the processing is based on a Data Subjects explicit consent.

Profiling per se which does not result in solely automated decisions is not prohibited.

6.8 RIGHT TO COMPLAIN

The HEA shall answer all data protection queries from staff, applicants, or other data subjects which relates to personal data held in the HEA. Any complaints received by the HEA relating to internal data protection procedures should be directed to the Data Protection Officer.

The Data Protection Officer will work with data subjects to bring complaints to a satisfactory conclusion for both parties. Data subjects will be informed of their right to bring their complaint to the Data Protection Commission and will be provided with the appropriate contact details.

6.9 RIGHT TO WITHDRAW CONSENT

Under Articles 4; 7 and 9 GDPR, the Data

Subjects have rights regarding consent and explicit consent. While the HEA may have obtained consent from Data Subjects to process their personal data for certain activities, Data Subjects may withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

A withdrawal of consent may still allow the processing of their personal data if there are other legal grounds for the processing, i.e. if:

- Processing is necessary for the performance of a contract to which the Data Subject is party
- Processing is necessary for compliance with a legal obligation
- Processing is necessary in order to protect the vital interest of the Data Subject or another natural person
- Processing is necessary for the performance of a task carried out in the public interest
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party[2]; except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

7 HOW TO EXERCISE YOUR DATA PROTECTION RIGHTS

As previously noted, Data Subjects have a number of rights under the GDPR. These rights can be applied by making a request to THE HEA using the appropriate link to the forms below.

DP Form 1: Subject Access Request

DP Form 2: Right to Rectification

DP Form 3: Right to Erasure

DP Form 4: Right to Restrict Processing

DP Form 5: Right to Data Portability

DP Form 6: Right to Object to Processing

DP Form 7: Right to Object to Automated Decision Making, including profiling

DP Form 8: Right to Withdraw Consent

To View these forms please click here

A Data Subject has the right to lodge a complaint with the Data Protection Commissioner, 21 Fitzwilliam Square S, Dublin 2, D02 RD28 (https://www.dataprotection.ie) with regards to the HEA processing of their personal data.

[2] This shall not apply to processing carried out by public authorities in the performance of their tasks.

7.1 HOW SOON WILL I GET A RESPONSE TO MY REQUEST

Data Subject requests will be responded to within one month as required by the Data Protection Law. The HEA may extend this period for up to 2 months if absolutely necessary and will inform the Data Subject if an extension is required.

The HEA will provide you with the personal information in a form which will be clear to the ordinary person (e.g., codes explained).

The HEA will provide personal information only to the individual concerned or someone acting on their behalf or with their authority. Personal information will not be given over the phone.

If no personal information is held about you, you will be informed of this within one month.

7.2 COST OF A REQUEST

As per the Data Protection Law, no fee applies to a request made by a Data Subject. However, the HEA may charge a reasonable fee for any additional copies of data requested by the Data Subject or where requests are manifestly unfounded or excessive.

8 TRANSFERRING PERSONAL DATA TO OTHER ORGANISATIONS

Organisations that transfer personal data from Ireland to third countries and other organisations for processing, i.e., places outside of the European Economic Area (EEA) need to ensure that there are adequate levels of data protection provided. When the HEA retains the services of an agent to process personal data on its behalf, we will put in place a contract in writing (or equivalent form) which deals adequately with issues of security, confidentiality and other data protection matters. With regard to the level of security measures that organisations must have in place to protect personal data, generally organisations must take all necessary and reasonable steps having regard to the state of current technology, and to the sensitivity of the personal data in question.

On some occasions, An Garda Síochána may ask HEA to provide information for the purposes of investigating a crime, pursuant to Section 41(b) of the Data Protection Act 2018. These requests should be documented on An Garda Síochána headed paper (official request – can be scanned & submitted), quote the explicit and specific data fields they require (minimisation), should also cite the legal basis for the request. he headed paper must be signed, by a Garda at the level of Superintendent or above.

9 WHO TO CONTACT IN THE HEA WITH REGARD TO DATA PROTECTION MATTERS

The Data Protection Officer,
Higher Education Authority,
3 Shelbourne Buildings,
Shelbourne Road,
Dublin D04 C2Y6

or by email to: dataprotection@HEA.ie.

10 RESPONSIBILITIES OF THE HEA

The HEA has responsibility for the following:

10.1 DATA PROTECTION BY DESIGN AND DEFAULT

The HEA will, at the time of determining the purposes for which personal data will be used as well as while using this personal data, implement appropriate technical and organisational measures to implement the data protection principles set out in this policy and integrate the necessary safeguards into all systems and applications which use personal data.

10.2 ESTABLISH APPROPRIATE AGREEMENTS WITH THIRD PARTIES

The HEA will implement appropriate arrangements, memoranda of understanding, bilateral agreements and contracts (collectively 'agreements') with all third parties with whom personal data is shared/processed.

10.3 TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EUROPEAN UNION

The HEA will not transfer personal data outside of the European Economic Area unless appropriate safeguards have been established and enforceable subject rights and effective legal remedies for data subjects are available.

10.4 MAINTAINING A RECORD OF PROCESSING ACTIVITIES

The HEA will maintain a record of processing activities detailing the processing activities which take place within the business, involving personal data.

This record of processing activities will be reviewed and signed off by Section Heads and equivalents at least every 6 months and will be made available to the Data Protection Commission on request.

10.5 PERSONAL DATA BREACHES A personal data breach is 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 by the HEA. The HEA will maintain procedures for handling data breaches. Such procedures will establish the methodology for handling a personal data breach and for the notification of the breach to the Data Protection Commission, third-party processors, and relevant data subjects, if necessary. The HEA has a separate breach Policy which is available on the staff intranet.

Where a type of processing, in particular using new technologies, and taking into account 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, the HEA shall undertake a DPIA prior to the commencement of processing.

The HEA will maintain procedures and documentation whereby a DPIA shall be conducted on all new types of processing, including the use of new technologies, that may result in a high risk to the rights and freedoms of any data subjects. This DPIA must be fully documented, and as part of this process, the Business Unit conducting the DPIA should seek the advice of the DPO. The DPO will provide advice where requested with regard to DPIAs and monitor their performance.

Where the HEA is unable to identify measures that mitigate the high risks identified through completion of the DPIA, the HEA will consult with the Data Protection Commission prior to the commencement of processing.

11 RESPONSIBILITIES OF STAFF (INCLUDING CONTRACTORS)

Any person who processes personal data on behalf of the HEA has a responsibility to comply with this policy and ensure compliance with the principles of data protection. All records created during duties carried out on the HEA's behalf are the property of the HEA and subject to its overall control.

Any person who processes the HEA's data will:

- Become familiar with and abide by any data protection policies, procedures and guidelines drawn up by the HEA;
- Endeavour to ensure that all data they access, manage and control as part of their daily duties is handled and maintained in accordance with data protection requirements;
- Return all such data held upon termination of their contract of employment, retiring or changing position within the HEA; and,
- Make efforts to comply with data protection obligations while processing personal data which is under the control of the HEA.

11.1 TRAINING

All staff are required to complete data protection awareness training. New staff will receive information and training as part of the induction process. Additional more in-depth training will be provided on a case by basis, depending on the data protection requirements of the post.

11.2 FAILURE TO COMPLY

The HEA takes compliance with this policy very seriously. If a staff member knowingly or wilfully fails to comply with any requirements, action may be considered under the HEA Code.

If staff consider that this policy has not been followed, they should raise the matter with their line manager or directly with the Data Protection Officer.

12 ROLE AND RESPONSIBILITIES OF THE DATA PROTECTION OFFICER

The HEA has appointed a Data Protection Officer (DPO) who reports directly to the Head of Corporate Affairs & Board/CEO. The DPO has been designated on the basis of professional qualities, in particular expert knowledge of data protection law. The HEA shall publish the contact details of the data protection officer and communicate them to the DPC.

The HEA shall ensure that the DPO is involved in all issues which relate to the protection of personal data processed by the HEA. The HEA shall support the DPO in performing the tasks referred to below.

The DPO shall have at least the following tasks:

- Inform and advise the HEA, individual business units, and staff of their obligations under data protection legislation;
- Monitor and audit compliance with data protection legislation and with the HEA's data protection policies across business units / sections of the HEA;
- Provide advice on the need to perform a data protection impact assessment and monitor the performance of any such assessments made;
- Co-operate with and act as a point of contact with the DPC;
- Determine if personal data breaches are reportable to the DPC;
- Be responsible for submitting completed breach notification forms to the DPC; and,
- Be a point of contact for data subjects seeking access to rights and provide advice and support to business units to ensure that the requests are responded to in accordance with the legislation.

The DPO shall have due regard to the risk associated with all data processing operations, considering the nature, scope, context and purposes of processing. This requires the DPO to prioritise his/her activities and focus efforts on issues that present higher data protection risks.

This approach will help the DPO to advise the HEA on the need for DPIAs, the areas which should be subject to internal or external data protection audit, the internal training activities required by staff or management responsible for data processing activities, and the processing operations which should be prioritised from a data protection perspective.

13 GLOSSARY

Term	Definition
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 Category 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.
Data Subject	The individual to whom some personal data relates.
Processing	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.
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.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Joint Controllers	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
Data Protection Officer	An appointed officer with responsibility for the Data Protection compliance of the organisation.
DPC	The Data Protection Commission.
GDPR	Regulation (EU) 2016/679—the General Data Protection Regulation.
DPIA	Data Protection Impact Assessment.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural

Term	Definition
	person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	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.
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.
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.
Genetic Data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Biometric Data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Data Concerning Health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Protection Statement- This statement can be added to forms, document, webpages etc when collecting information from data subjects.

"The Higher Education Authority may require stakeholders to provide certain personal data in order to carry out its functions. The HEA will at all times process personal data in line with GDPR and the Data Protection Act 2018. More detail can be found in our Data Privacy Notice, which is available on our website, or in hard copy on request."