Policy Title:	Data Protection Policy and Procedures
Description:	This document states the policy and procedure at Marino Institute of Education to safeguard individuals' rights and freedoms in relation to personal data of Staff, Students, and others who engage with the Institute.
Author (Position):	Data Protection Officer
Version:	1.1
Approved By:	Governing Body
Policy Approval Date:	November 2023
Date of Next Policy Review:	June 2027 (or as necessary)

Contents

Data Protection Policy and Procedures

1. Context

Marino Institute of Education (hereinafter referred to as 'MIE') is required to collect personal information for a variety of purposes related to its core functions and activities. This data relates to Students, Staff and other persons who are associated with the Institute (ref Appendix 1). In addition, MIE may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the Irish and European legislation and regulations including, General Data Protection Regulation (GDPR) EU 2016/679, Data Protection Directive 95/46/EC, European Communities (Data Protection) Regulations, 2001, and the relevant Data Protection Acts which seeks to safeguard the privacy rights of individuals, and any other relevant data protection laws and codes of conduct (herein collectively referred to as 'data protection laws').

MIE fully respects an individual's right to privacy and is committed to preserving the rights of those who share information with the Institute. Any personal information that is processed by MIE is treated with the highest standards of security and confidentiality, in accordance with the data protection laws.

MIE has developed policies, procedures, controls and measures to ensure continued compliance with the legislation, including staff and student training, policy and procedure documents, processing records, audit measures and assessments[1]. Ensuring and maintaining the security and confidentiality of personal data is a core priority. MIE is proud to operate a 'Privacy by Design' approach (see Section 17), assessing changes and their impact from the outset and designing systems and processes to protect personal information throughout the processing cycle.

2. Purpose

The purpose of this policy is to assist MIE in meeting its legal, statutory and regulatory requirements under the data protection laws, and to ensure that all personal information

[1] See MIE Information Compliance

under the control of the Institute is processed in a compliant manner and in the individual's best interest.

Data protection laws include provisions that promote accountability and governance and, as such, MIE has put comprehensive and effective governance measures in place to meet these provisions. The aim of such measures is to minimise the risk of breaches, and to uphold the protection of personal data. This policy also serves as a reference document for Staff, Students, and third parties on the responsibilities of processing personal data which is under the control of the Institute.

3. Objectives

MIE is committed to ensuring that all personal data processed by the Institute is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

MIE has developed the following objectives to meet our data protection obligations and to ensure continued compliance with legal and regulatory requirements.

MIE ensures that:

- We protect the rights of individuals with regards to the processing of personal information;
- We develop, implement and maintain a data protection policy, procedure, audit plan and training programme for compliance with the data protection laws;
- Every practice, function and process carried out by MIE, is monitored for compliance with the data protection laws and its principles;
- Personal data is only processed where we have verified and met the lawfulness of processing requirements;
- We only process special category data in accordance with GDPR requirements;

- We record consent at the time it is obtained[2] and evidence such consent to the Data Protection Commission (DPC), where requested;
- All staff are aware of their GDPR obligations and are provided with training in data protection laws, principles, regulations and how they apply to their specific role at MIE;
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws;
- We maintain a continuous programme of monitoring, review and improvement with regard to compliance with data protection laws and strive to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary;
- We monitor the DPC, European Data Protection Board and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements;
- We have robust and documented data breach controls and complaint handling for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection;
- Our Data Protection Officer (DPO) is responsible for the overall supervision, implementation and ongoing compliance with data protection laws, and performs specific duties as set out under Article 37 of the GDPR;
- We have an auditing and monitoring programme in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared[3]. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance[4];
- We provide clear reporting lines and supervision with regard to data protection. We store and destroy all personal information, in accordance with our retention policy and

[2] See Record Management Policy and MIE Records Retention Schedule

[3] See MIE Privacy Statement, Record Management Policy and MIE Records Retention Schedule

[4] See MIE Data Protection

schedule[3] which has been developed from the legal, regulatory and statutory requirements and suggested timeframes.

- Any information provided to an individual in relation to personal data held or used about them is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- Employees are aware of their own rights under the data protection laws, and are provided with the Article 13/14 information disclosures in the form of the MIE Privacy Statement;
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements;
- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust information security programme in place.

4. Scope

This policy applies to all Students and Staff within MIE (including, but not limited to, permanent, fixed term, and temporary staff, third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with MIE) and relates to the processing of personal data on behalf of the Institute at all locations where MIE-controlled personal data is processed, including remote working or working from home. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action[5].

5. Data Protection Notice

MIE fully respects your right to privacy and actively seeks to preserve the privacy rights of those who share information with the Institute. Any personal information which you volunteer to the Institute will be treated with the highest standards of security and confidentiality, in accordance with Irish and European Data Protection legislation. Personal

[5] See Disciplinary Policy and Disciplinary Procedures in Respect of Students

data will be processed shall in accordance with the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018. See MIE Privacy Statement.

6. Definitions

6.1. Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

6.2. Data Breach: Under GDPR, a personal data breach is defined as 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. This definition extends to breaches which result from, malicious conduct, lack of appropriate security controls, system or human failure, or error.

6.3. Data Controller: means 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 EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

6.4. Data Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

6.5. Data Protection Laws: means, for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws with which MIE complies.

6.6. Data Subject: means 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.

6.7. GDPR: means the GDPR EU 2016/679.

6.8. **Personal Data:** means any information relating to an identified or identifiable natural person (see Data Subject Access Request (SAR) Policy). Personal data may be processed in paper and electronic form. Information protected under the GDPR is known as 'personal data' and is defined as:

'Any information relating to an identified or identifiable natural person; 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.' Examples of personal data are listed in Appendix 1.

6.9. **Processing:** means 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.

6.10. **Recipient:** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing.

6.11. **Special Categories of Personal Data:** refers to those categories of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, and which merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms of an individual.

This data is categorised under GDPR as any of the following:

- Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade-union membership;

- The processing of genetic data for the purpose of uniquely identifying a natural person;
- The processing of biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health;
- Data concerning a natural person's sex life or sexual orientation.

In relation to the 'special categories of personal data', the GDPR advises that: 'Processing of 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 shall be prohibited – unless one of the Article 9 clauses applies.'

6.12. Supervisory Authority: means an independent public authority which is established by a Member State. In Ireland, the Supervisory Authority is the DPC.

6.13. Third Party: means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

7. GDPR Principles

MIE must adhere to the principles of personal data processing, as set out in GDPR Article 5(1). Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency');***

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with GDPR Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 in accordance with GDPR Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation');*** and

f) 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, using appropriate technical or organisational measures ***('integrity and confidentiality')***.

GDPR Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ***('accountability')*** and requires that controllers such as MIE show how they comply with the principles, detailing and summarising the measures and controls that are in place to protect personal information and mitigate risks associated with processing.

8. Data Protection Legislation

The General Data Protection Regulation (GDPR) EU 2016/679 applies to all EU Member States since 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation. As MIE processes personal information regarding individuals (*data subjects*), the Institute are obligated under the GDPR to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles:

- EU General Data Protection Regulation 2016 (GDPR) Data Protection Act 2018;

- S.I. No. 314 of 2018 - Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 Universities Act, 1997;
- Data Sharing and Governance Act 2019;
- Higher Education Authority Act, 1971.

9. Legal Basis for Processing ('Lawfulness')

In order to process personal data lawfully, MIE must have a legal basis for doing so. There are six legal bases for processing personal data, of which no single basis is preferred or regarded as more significant than another. The basis that is regarded as most appropriate will depend on the purpose of the processing, and MIE's relationship with the individual.

9.1. The six legal bases as set out in Article 6(1) GDPR are:

1. Consent: The individual has (freely) given clear, specific, informed and unambiguous consent for MIE to process their personal data for a distinct purpose;
2. Contractual Basis: The processing is necessary for a contract which MIE has with the individual, or because they have asked the University to take specific steps before entering into a contract;
3. Legal Obligation: The processing is necessary for MIE to comply with Irish and EU law;
4. Vital Interests: The processing is necessary to protect the life of an individual;
5. Public Interests: The processing is necessary for MIE to perform a task in the public interest or for the purpose of its statutory functions. MIE provides the Higher Education Authority with anonymised socioeconomic data and first employment destination data.
6. Legitimate Interests: The processing is necessary for the legitimate interests of MIE or a third party. Where we rely on this lawful basis, MIE will conduct a legitimate interest assessment to ensure said interests are balanced against the interests of the data subjects in question.

MIE is required to determine the most appropriate legal basis before processing personal data in a specific context and should document the legal basis in relevant Privacy Statements[6].

9.2. Consent

In cases where MIE relies on consent as a lawful basis for processing personal data, the Institute must:

- obtain an individual's specific, informed and freely given consent;
- ensure that the individual gives consent by a statement or a clear affirmative action and document the statement or affirmative action; and
- allow an individual to withdraw their consent at any time without detriment.

Where consent is obtained verbally, it is strongly recommended that Staff/Students utilise scripts and checklists approved by the Data Protection Officer to ensure that all necessary requirements have been met and that consent is obtained compliantly and can be evidenced.

10. Processing Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies are being updated to ensure that employees are provided with the appropriate information disclosure, and are aware of how we process their data and why. All employees are provided with a Privacy Notice specific to the personal information we collect and process about them.

11. Processing Special Category Data

When processing special categories of data (see Section 6.11, sensitive data), it is necessary for the processing to be covered both by a legal basis under GDPR Article 6 and by a special category condition set out under GDPR Article 9.

[6] See MIE Privacy Statement

Where MIE processes any personal information classed as special category, we do so in accordance, with GDPR Article 9.

Special category data is only processed where:

- The data subject has given explicit consent to the processing of the personal data;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law;
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- Processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Processing is necessary for reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 89(1).

Where MIE processes personal information that falls into one of the above categories, adequate and appropriate provisions and measures are in place prior to any processing. Measures include*:*

- Verifying our reliance on GDPR Article 9(1) prior to processing;

- Documenting the GDPR Article 6(1) legal basis relied upon from processing on our Processing Activities Register encompassed within our GDPR logs (see GDPR Article 30) (where applicable);
- Having an appropriate policy document in place when the processing is carried out, specifying our:
  - Procedures for securing compliance with the data protection laws principles;
  - Policies as regards the retention and erasure of personal data processed in reliance on the condition;
  - Retention periods and reason (ref Data Retention & Erasure Policy);
  - Procedures for reviewing and updating our policies in this area[7].

12. Records of Processing Activities (RoPAs)

With reference to the type of data processed at MIE (ref GDPR Article 30), records of processing activities involving personal data are maintained (in writing) in a clear and easy to read format that are readily available to the Supervisory Authority upon request.

Acting in its capacity as a data controller, MIE's internal records of processing activities carried out under the control of the Institute contain the following information:

- The Institute's name and contact details, and the name and contact details of the DPO.
- Where applicable, MIE also records joint controller details and/or details pertaining to the controller's representative;
- The purposes of the processing;
- A description of the categories of data subjects;
- The categories of personal data;
- The categories of processing carried out on behalf of each controller;
- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations);

[7] See Record Management Policy and MIE Records Retention Schedule

- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards);
- Where possible, the envisaged time limits for erasure of the different categories of data;
- A general description of the processing security measures pursuant to GDPR Article 32(1).

13. Third Party Processors

MIE utilises the services of third parties for certain processing activities. The Institute engages in due diligence (e.g. Data Protection Impact Assessment). We ensure that we havethe appropriate contractual arrangements in place (e.g. Data Protection Agreement and Data Sharing Agreement) when forming business relationships and use information audits to identify, categorise and record personal data that is processed outside MIE's direct control, so that the data, processing activity, processor and legal basis are recorded, reviewed and easily accessible.

Such external processing includes (but is not limited to):

- IT systems and services
- Human Resources
- Student Support Services (Counselling Service, Disability Service, Medical Service)
- Payroll
- Legal services (including the Counselling Service, the Disability Service and the Medical Service, with all of whom MIE has service level agreements).

The continued protection of data subject rights and the security of personal data is prioritised when choosing a processor. MIE recognises the importance of adequate and reliable outsourcing for processing activities as well as the Institute's continued obligations under data protection legislation for data processed by a third party. MIE ensures that processing is limited to third parties operating under formal agreements which satisfy the requirements of Article 28 of the GDPR.

We have strict due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, and references, and ensure that the processor is adequate, appropriate and effective for the task for which we are employing them. Their processes and activities are audited prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We draft bespoke Service Level Agreements and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that detail:

- The processors data protection obligations;
- Our expectations, rights and obligations;
- The processing duration, aims and objectives;
- The data subjects' rights and safeguarding measures;
- The nature and purpose of the processing;
- The type of personal data and categories of data subjects.

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor:

- Processes the personal data only on our documented instructions;
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject);

- Shall inform us of any such legal requirement to transfer data before processing;
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Takes all measures to security the personal data at all times;
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights;
- Assists the Institute in ensuring compliance with our obligations for data security, mitigating risks, breach notification (I would recommend that your 3rd parties are obligated to notify you, MIE, of any breaches that they become aware of within the first 24 hours of its occurrence) and privacy impact assessments;
- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible;
- Makes available to the Company all information necessary to demonstrate compliance with the obligations set out in the agreement and contract;
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract;
- Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract.

14. Data Subject Rights

Under GDPR Chapter III, MIE is required to ensure a number of rights for individuals[8]

14.1. The Right to be Informed (GDPR, Article 13 and 14)

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR. Where personal data

[8] See MIE Privacy Statement

is being collected directly from an individual, a Privacy Statement/Notice must be provided at the point at which the data is collected.

This is a sample statement which describes how MIE intends to process personal data, and must contain the following information:

- Who is collecting and processing the data (e.g. Department in MIE);
- Why the data is being processed;
- The legal basis used to justify the processing;
- The format of the processing;
- How long the data will be retained;
- To whom will the data be disclosed;
- Individuals' rights under data protection law (access, erasure, objection, etc.).

14.2. The Right of Access (GDPR, Article 15)

Data subjects are entitled to make an access request for a copy of their personal data and for information relating to that data. This data request must be complied-with within one month. Such information must be provided free of charge and in writing, or by other means where authorised by the data subject.

Individuals wishing to make a request to access their personal data are advised to complete **MIE Data Subject Access Request (SAR) Form**. Access requests should be forwarded to MIE's DPO as soon as received and a record of the request should be noted on PrivacyEngine.

Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances, and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay. Where MIE does not comply with a request for data provision, the data subject must be informed within one month of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority, the DPC.

Please refer to MIE's **Data Subject Access Request (SAR) Policy** for guidance on how an access request should be fulfilled.

14.3. The Right to Rectification (Correcting Inaccurate or Incomplete Data) (GDPR, Article 16 and 19)

Under GDPR Article 5 (1)(d), personal data processed by MIE should be reviewed and verified as being accurate wherever possible. Where inconsistencies are identified by MIE, or where a data subject or other party informs the Institute, every reasonable step should be taken to ensure that such inaccuracies are corrected with immediate effect.

All requests for rectification of personal data should be forwarded to the DPO without delay.

14.4. The Right to Erasure (GDPR, Article 17)

The right to erasure, whereby individuals can petition an organisation to have their data erased from its systems, is also known as 'the right to be forgotten'. The right to erasure is not absolute and only applies in certain circumstances. MIE must respond to a request within one calendar month.

All requests for erasure of personal data should be notified to the DPO without delay.

14.5. The Right to Restrict Processing (GDPR, Article 18)

There may arise certain circumstances whereby MIE may be required to restrict the processing of personal data, to validate, verify or comply with a legal requirement of a data subject's request. Restricted data should be removed from the normal flow of information and recorded as such. The right to restrict processing is not absolute and only applies in certain circumstances. MIE must respond to a request within one calendar month. All requests for restriction of processing should be notified to the DPO without delay.

14.6. The Right to Object to Processing (GDPR, Article 21)

Data subjects should be informed of their right to object to processing in MIE Privacy Statements[9] and at the point of first communication, in a clear and legible form and

[9] See MIE Privacy Statement

separate from other information. In addition, MIE provides opt-out options on all direct marketing material, whether conducted by MIE or by third parties on the Institute's behalf.

Data subjects have the right to object to:

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for purposes of scientific/historical research and statistics.

Where MIE processes personal data for the performance of a legal task, in relation to the legitimate interests of the Institute or for research purposes, a data subject's objection will only be considered where it is on grounds relating to their particular situation. MIE reserves the right to continue processing such personal data where:

- The Institute can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Where a data subject objects to processing on valid grounds, MIE will cease the processing for that purpose and advise the data subject of cessation in writing within one month of the objection being received.

In the event that MIE uses automated decision-making processes, the Institute must inform the individual of same, and advise them of their rights. MIE must also ensure that individuals can obtain human intervention, express their point of view, obtain an explanation of the decision, and challenge it.

All requests regarding an objection to processing should be notified to the DPO without delay.

14.7. The Right to Data Portability (GDPR, Article 20)

The right to data portability allows data subjects to manage their personal data for their own purposes across different platforms and services. Data portability facilitates data

subjects to transmit personal data from one IT environment to another without hindrance to usability.

The right to data portability is not absolute and applies in the following circumstances only:

- To personal data that a data subject has provided directly to a controller;
- Where the processing is based on consent or for the performance of a contract; and
- When processing is carried out by automated means.

All transmission requests under the portability right should be assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the data subject requesting the transmission to another controller, this is always to be effected without prejudice to the rights and freedoms of the other data subjects. All requests received regarding data portability should be forwarded to the DPO.

Data subjects also have a right to complain to a relevant supervisory authority. The contact details for the DPC are as follows:

- Telephone: +353 578 684 800;
- Online: Data Protection Commission - contact

A data subject and may exercise any of these rights at MIE by contacting the Institute's DPO (dpo@mie.ie).

15. Data Security

Under GDPR Article 32, individuals processing personal data on behalf of MIE must take appropriate measures to preserve data security and mitigate risk in order to safeguard personal data which is under the control of the Institute.

Examples of breaches of security include:

- Unauthorised access to or use of MIE-controlled personal data
- Inappropriate access controls facilitating unauthorised use or disclosure of the data
- Loss of data
- Theft of data

- Data being altered, deleted or destroyed without authorisation
- Attempts to gain unauthorised access to MIE-controlled computer networks and systems; e.g. hacking and Computer viruses or other security attacks, e.g. ransomware, phishing, malware, etc.

  GDPR requires that the following technical and organisational measures are implemented as appropriate:
- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- The implementation of processes to regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing.

  In addition, GDPR Article 32 requires that "*in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing*".

  The DPC has published Guidance on Controllers and Data Security.

  Comprehensive information on MIE's IT security provisions, including IT security policies, email security, cloud computing, training, backups and encryption is available from MIE IT Security Policy and MIE Policy on Cloud Computing Services.

16. Breaches of Personal Data Security

MIE has implemented robust and documented complaint handling and data breach controls for identifying, investigating, reviewing and reporting breaches or complaints. All Staff and Students in MIE must adhere to the MIE Staff & Students Code of Conduct for Use of IT Systems, Disciplinary Policy and Disciplinary Procedures in Respect of Students to assist staff in identifying and handling incidents involving personal data breaches.

MIE staff are required to take all necessary steps to reduce the impact of incidents involving personal data. Where a data breach is likely to result in a risk to the rights and freedoms of data subject, the DPO will liaise with the DPC and report the breach within 72 hours of becoming aware of the existence of a breach. (see GDPR Article 33). The DPO will also recommend, where appropriate, actions to inform data subjects and reduce risks to their privacy arising from the breach, (see GDPR Article 34).

Staff, students and contractors who discover a personal data breach or incident should immediately inform their Head of Department who should contact the DPO, in line with the MIE Staff & Students Code of Conduct for Use of IT Systems.

17. Data Protection by Design and Default

GDPR Article 25 provides for two crucial concepts for future project planning: Data Protection By Design and Data Protection By Default.

Data Protection by Design: Controllers must ensure that privacy-enhancing considerations and technologies are considered from the outset, and for the entirety of the lifecycle thereafter, of a system, project or process. This will help to ensure stronger protection for individual data privacy when processing personal data.

Data Protection by Default: Controllers must apply privacy settings as standard to a particular process, product or service from the outset of availability to individuals, without any manual input from the end user.

MIE staff must apply the principles of Data Protection by Design and by Default when processing personal data. This can be attained by:

- Performing a Data Protection Impact Assessment (DPIA) in instances where processing is likely to result in a high risk to the rights and freedoms of individuals, particularly when new technologies are being used to process data;
- Performing a DPIA where systematic and extensive evaluation of individuals is to be carried out based on automated processing, including profiling, or where the processing relates to large scale processing of special categories of data/personal data relating to criminal convictions;

- Performing a DPIA when processing involves the large-scale systematic monitoring of individuals of a publicly accessible area (e.g. MIE Campus Security CCTV systems)
- Processing the minimum amount of required personal data for the minimum amount of time necessary for the purpose;
- Anonymising or pseudonymising personal data where necessary and appropriate, including for research purposes.

18. Data Protection Impact Assessment

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by MIE. The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation by systematically identifying and minimising potential privacy risks as early as possible, and devising suitable mitigation measures (see GDPR Article 35(3)). It also provides evidence that the risks to individuals have been considered, and sufficient measures have been taken to protect those individuals. The DPIA should assess the activity to be carried out against the Principles of Data Protection (see Section 7) and determine whether the processing of personal data is both necessary and proportionate, or whether changes to the process or additional controls are required.

The DPIA methodology enables controllers to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA, and risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either:

- Eliminated
- Reduced
- Accepted.

19. CCTV

CCTV systems are installed on MIE premises to provide for the protection, safety & security of MIE students and staff and all visitors to the property. In addition, the purpose of CCTV at MIE is to facilitate proceedings in the context of criminal or legal issues, including the investigation of major staff, student or visitor disciplinary offences. CCTV cameras may

also be used for purposes other than security, for example as part of a research project, for the purpose of recording the progress of a large building project or for monitoring the performance of important items of equipment or machinery.

When using CCTV systems, MIE will have the greatest possible regard for the protection of the fundamental right to privacy enjoyed by each staff and student member of the Institute, as well as visiting members of the public, and their rights of free association and free expression within the law. CCTV cameras will not be used with the intention of monitoring or recording Students' Union activities at MIE. Those charged with the operation of the various CCTV systems must exercise the greatest possible care, and ensure that the systems are not used in any unauthorised or inappropriate manner. Installation of a CCTV system at the MIE must involve consultation with the Conferencing and Facilities Department and the DPO, and a DPIA must be undertaken.

Further information is available in MIE's CCTV Policy, and in MIE Privacy Statement. Guidance on the use of CCTVsystems is available from the DPC.

20. Data Retention and Destruction

MIE adheres to the GDPR requirement to process personal data for as long as is necessary. In so doing, the Institute has defined procedures for adhering to statutory retention periods as set out by legislation, as well as those periods stipulated under contractual requirements,

Personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

Please refer to Record Management Policy and MIE Records Retention Schedule for full information on MIE's defined retention periods and archiving and destruction processes.

21. GDPR Awareness and Training at MIE

MIE provides an online GDPR training programme for staff and students. The programme is available through the Institute's online platform, and includes a number of courses each with individually focused modules.

Our online programme for staff includes:

- Mandatory courses for all staff
- Selected courses for specific departments, projects, etc.
- Occasional courses, e.g. optional course on cyber security at home.

The minimum mandatory training time for staff is 130 minutes, which includes

- Overview of the main requirements of GDPR for organisations, types of data which need to be protected under the regulation, roles and responsibilities of the Data Controller and the Data Processor, key principles of Lawfulness and Accountability, individual rights guaranteed by GDPR, as well as practical precautions that staff can take and the procedure to follow in the event of a data breach.
- Cybersecurity Awareness aims to ensure a minimal risk of cyber-attacks and data breaches occurring at the Institute and includes a description of typical forms of malware that currently hit organisations, explains how to create safer internet use, data storage and personal devices. It includes a brief introduction to GDPR, the Data Protection Act and other legislation which regulates issues over data breaches and information security.
- Data Subject Access Request (DSAR) and Data Breach courses which offer a detailed breakdown of how to complete the steps involved when dealing with data subject access requests (DSARs), including explaining the requirements for a valid DSAR and handling third party personal data, and explains a data breach and the related GDPR obligations and duties as well as the steps to be followed in the situation of a data incident or data breach.

Selected courses are completed by teams, departments, committees, projects, etc as required and may be coordinated by the DPO or Data Champions within departments, e.g.

- Data Protection Impact Assessment (DPIA) – Why? How? (Leadership Team, Data Champions)
- Data Protection by Design and Default (Data Champions)

- GDPR and Children (MERC)

An online GDPR training programme for students includes general GDPR awareness, as well as bespoke courses, e.g. relating to research projects, pre-placement in school or other education settings. All courses are available through MIE's online platform.

Occasional optional courses are offered to staff and/or students, e.g. cyber security at home to address authentication factors, social media, online shopping, phishing, ransomware, etc.

22. Data Protection Officer (DPO)

As a public authority, MIE is required to appoint a DPO, as per Article 37(1)(a). The role of the DPO is:

- To advise the Institute and its staff regarding their responsibilities under data protection legislation;
- To monitor compliance with data protection legislation and relevant policies;
- To provide training and increase awareness among staff;
- To provide guidance on the completion of DPIA;
- To co-operate and act as the contact point with the DPC in relation to complaints, investigations, audits and consultations and any other matter relevant to the legislation.

Contact details for the DPO at MIE are:

By email: dpo@mie.ie

By An Post:

Data Protection Officer,	Oifigeach Cosanta Sonraí,
Marino Institute of Education,	Institiúid Oideachais Marino,
Griffith Avenue,	Ascaill Uí Ghríofa,
Dublin 9, D09 R232	Baile Átha Cliath 9, D09 R232
Ireland.	Éire.

22.1. Data Champions

Data Champions, who are nominated within Departments throughout MIE, have a central role in effective data protection at GDPR implementation at MIE. Working closely with the DPO, the role of the Data Champion is

- To promote good data management and coordinate Data Protection compliance matters within their area of responsibility;
- To be a point of contact for the DPO regarding Data Protection matters;
- To identify and address organisational risks, as well as actions to mitigate and reduce future risks;
- To bring relevant Data Protection/GDPR to the attention of staff in their area.

22.2. Document Reviewers

The role of Document Reviewer is held by members of the Leadership Team, and other members of staff who assist in the process of Data Protection and GDPR policy and procedure development as designated from time to time.

22.3. Data Protection Consultancy

MIE's GDPR compliance is supported by PrivacyEngine, an independent data protection consultancy offering specialist services regarding compliance with the Irish and EU Data Protection legislation. MIE uses its online portal, PrivacyEngine, to consolidate and manage GDPR material, and to comply with the specific GDPR obligations.

23. Data Protection Commission

The DPC is the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The Commission is the Irish supervisory authority for the GDPR, and has functions and powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the Health Research Regulations (2018).

Further information on how the DPC safeguards and regulates data protection rights for individuals and responsibilities for data controllers, as well as general guidance on data protection is available at https://www.dataprotection.ie/.

Contact details for the DPC:

21 Fitzwilliam Square South,

Dublin 2, D02 RD28,

Ireland.

Telephone: +353 761 104 800

Webform: https://forms.dataprotection.ie/contact

24. Related Documents

24.1. MIE Staff & Students Code of Conduct for Use of IT Systems

24.2. MIE Disciplinary Policy

24.3. Disciplinary Procedures in Respect of Students

24.4. MIE Privacy Statement

24.5. Record Management Policy

24.6. MIE Records Retention Schedule

24.7. MIE Data Protection Subject Access Request Policy and Procedures

24.8. MIE Data Subject Access Request (SAR) Form – Garda Síochána

24.9. MIE Data Breach Policy and Procedures

24.10. MIE Data Breach Incident Form

24.11. Data Protection Impact Assessment (DPIA)

24.12. CCTV Policy

Appendix 1 - Personal Data collected by MIE (Staff and Students)

CONTEXT FOR DATA COLLECTION AT MIE - STAFF		
Category of data	**Purpose for processing**	**Legal basis (ref GDPR Article 6/9)**
Names	Processing is necessary due to the fulfilment of the employment contract and also necessary to comply with the law and revenue requirements.	Article 6 (Contract/Legal Obligation)
Home address	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements.	Article 6 (Contract/Legal Obligation)
Home phone/mobile phone number	Contact numbers are collected to enable the processor contact the employee should there be any queries or follow-ups on contracts or payments required.	Article 6 (Consent)
Personal email address	The email address is used to send and receive information to the CORE payroll/HR system.	Article 6 (Contract/Consent)
Date of Birth/Age	This information is required to ensure compliance with employment laws and to ensure the correct taxation rates are applied to the schedule E income.	Article 6 (Legal Obligation)
Birthplace/citizenship/nationality	This information is required to ensure compliance with employment laws and to ensure the correct taxation rates are applied to the schedule E income.	Article 6 (Legal Obligation)
Marital status	This information is collected for the purpose of Death in Service Benefit which applies different rates to married and single people. This information is collected for INVESCO a third party who manages the MIE Pension Schemes.	Article 6 (Contract/Consent)
PPS number	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements.	Article 6 (Contract/Legal Obligation)
MIE ID number	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements.	Article 6 (Contract/Legal Obligation)

Next of kin/dependent/family details	Persons to be contacted in case of an emergency.	Article 6 (Consent)
Photographs	Images may be used in MIE publications, e.g. newsletters and brochures, on display boards, in electronic versions of publications, and on the MIE websites or other electronic forms of media. These images are retained for as long as required for the purposes outlined above (ref MIE Retention Schedule).	Article 6 (Legitimate interests/ Consent)
Curriculum Vitae	For permanent staff, all CVs are kept on file. CVs of unsuccessful candidates are destroyed (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Personal financial data – bank account	Processing is necessary due to the fulfilment of the employment contract.	Article 6 (Contract)
Details of gifts donations made	Date is collected to comply with revenue guidelines on gifts and donations made to staff.	Article 6 (Legal Obligation)
Income/salary	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements.	Article 6 (Contract/Legal Obligation)
CCTV images	Data is processed in line with CCTV Policy, and with reference to MIE Retention Schedule.	Article 6 (Legitimate interests)
Video images, including identifiable individuals	Video images may be used for presentations, lectures, instruction guidelines, etc on MIE websites or other electronic forms of media. These recordings are retained for as long as required for the purposes outlined above (ref MIE Retention Schedule).	Article 6 (Legitimate interests)
Voice recordings	Voice recordings may be used for presentations, lectures, instruction guidelines, etc on MIE websites or other electronic forms of media. These recordings are retained for as long as required for the purposes outlined above (ref MIE Retention Schedule).	Article 6 (Legitimate interests)
Employment history	For permanent staff, information is kept on file. Information re unsuccessful candidates is destroyed (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Sick leave details/medical certificates	Collected and retained by HR department (ref MIE Retention Schedule).	Article 9 (Contract/Legal Obligation)
Other leave data (excl. sick leave)	Collected and retained by HR department (ref MIE Retention Schedule).	Article 6, 9 (Contract/Legal Obligation)
Qualifications/Education Details	For permanent staff, such information is kept on file. Information re unsuccessful candidates is destroyed (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Work performance	Collected and retained by HR department (ref MIE Retention Schedule).	Article 6

		(Contract/Legal Obligation)
References	Such data is collected, and referees may be contacted. For permanent staff, such information is kept on file. Information re unsuccessful candidates is destroyed (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Grievance/Disciplinary details	Collected, and retained for the duration of the process and any sanction (ref MIE Retention Schedule).	Article 6, 9 (Contract/Legal Obligation)
Examination/assignment results	Collected and retained by HR department (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Professional association membership	Collected and retained by HR department (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Signatures (incl Electronic)	Used on a regular basis as part of arrangements due to COVID-19 restrictions. Collected by HR department (ref MIE Retention Schedule).	Article 6 (Legitimate interests/ Consent)
CPD records	May be collected and retained by HR department (ref MIE Retention Schedule).	Article 6 (Contract/Legal Obligation)
Car registration details	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements. (Mileage Calculations and Cut Offs)	Article 6 (Contract/Legal Obligation)
Location data	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements. (Taxation of non-residence and individuals outside of the EU)	Article 6 (Contract/Legal Obligation)
Data relating to children	Processing is necessary due to the fulfilment of the employment contract and necessary to comply with the law and revenue requirements. (Parental Leave, Maternity Leave, Parents Leave, Paternity Leave, Parents Leave & Pensions.	Article 6 (Contract/Legal Obligation)

CONTEXT FOR DATA COLLECTION AT MIE – STUDENTS (including IFP)		
Category of data	**Purpose for processing**	**Legal basis (ref GDPR)**
Names	To be able to address students and determine one from another.	Article 6 (Contract/Legal Obligation)
Home address	To write to students with information such as exam transcripts.	Article 6 (Contract/Legal Obligation)
Home phone/mobile phone number	To contact students in various circumstances (e.g. in relation to illness)	Article 6 (Consent)

Nationality	For purposes of registration	Article 6 (Contract/Legal Obligation)
Degree Choice	For purposes of registration	Article 6 (Contract/Legal Obligation)
Personal email address	To contact students between the time they are offered a place and the time they register. After graduation, students are copied on this e-mail address to ensure that information is received.	Article 6 (Contract/Consent)
Date of Birth/Age	To know if a student is under or over 18 (e.g. Garda vetting) and under or over 23(for mature student entry). Can also be used to verify identity when a student seeks sensitive information by phone.	Article 6 (Legal Obligation)
Birthplace/citizenship/ nationality	Is collected to determine appropriate fee to be charged.	Article 6 (Legal Obligation)
Gender	Is collected so that the correct salutation is used in the event that gender is not apparent from a first name and for returning data to the HEA.	Article 6 (Contract/Legal Obligation)
Marital status	Not routinely collected, but may be required if a student is seeking a grant or other support whereby family circumstances or means is a criterion for such support.	Article 6 (Contract/Consent)
PPS number	Collected as a unique identifier of students, and required by HEA and SUSI.	Article 6 (Contract/Legal Obligation)
National ID Card details	Not routinely collected, but Civil ID number may be required for some international students to allow for invoicing to embassy, etc.	Article 6 (Contract/Legal Obligation)
MIE ID number	Students are assigned a student number (for communication, incl with TCD re graduation), and exam number and a seat number (for anonymous marking of exam papers).	Article 6 (Contract/Legal Obligation)
Next of kin/dependent/family details	Information is collected in the event that a student's family needs to be contacted in the event of an emergency (e.g. injury or illness). It may also be collected by the Finance Office if next of kin members are paying student fees.	Article 6 (Consent)
Disability details	Required in order to register the student with the disability service.	Article 6, 9 (Consent/Contract/Legal Obligation)

Passport Details	Is collected to determine appropriate fee to be charged (international students)	Article 6 (Contract/Legal Obligation)
Curriculum Vitae	Not usually collected, but may be submitted by students to support application for some courses.	Article 6 (Contract/Legal Obligation)
Photographs	Collected for student cards and identification of students at exam courts.	Article 6 (Contract/Legal Obligation)
Employment history	Not routinely collected, but such information may be submitted for PME/ postgraduate entry to allow interview panel to assess candidate suitability for a course.	Article 6 (Contract/Legal Obligation)
Sick leave details/medical certificates	Collected only if a student is absent from classes or if a student is seeking a deferral or other discretion on medical grounds (e.g. in an academic appeal)	Article 6, 9 (Contract/Legal Obligation)
Other leave data (excl. sick leave)	If a student is absent from class, the reason for this is sought for accountability purposes in line with attendance policy and on compassionate grounds (e.g. where a student may be experiencing difficulties in engaging with the course).	Article 6, 9 (Contract/Legal Obligation)
Qualifications/Education Details	Is sought to assess candidates' suitability for a course.	Article 6 (Contract/Legal Obligation)
Work performance	Not routinely sought, but may be submitted in a reference.	Article 6 (Contract/Legal Obligation)
Financial Payment Guarantee Letters	Collected from some international students for the purpose of invoicing their embassy.	Article 6 (Contract/Legal Obligation)
References	May be submitted as part of an application for a course but is not routinely sought in most cases (but is sought from students seeking advanced entry or alternative entry routes).	Article 6 (Contract/Legal Obligation)
Grievance/Disciplinary details	Is collected only if a student is the subject of a complaint in light of Dignity and Respect Policy or disciplinary procedures.	Article 6, 9 (Contract/Legal Obligation)
Examination/assignment results	Collected to report results to students, and from applicants to determine eligibility for entry to a course.	Article 6 (Contract/Legal Obligation)
Individual Student Performance	To confirm if students have met requirements for progression to undergraduate study in TCD or to receive their certificate.	Article 6 (Contract/Legal Obligation)

Professional association membership	Not routinely sought, but may be submitted by candidates to support a course application.	Article 6 (Contract/Legal Obligation)
Signatures (incl Electronic)	Is sought so that it can be included on student cards.	Article 6 (Contract/Legal Obligation)
Personal financial data – bank account	Details may be collected by the Finance Office to provide payments to students who are eligible for support under various schemes, or for fee and accommodation refunds.	Article 6 (Contract/Legal Obligation)
Income/salary	May be collected to determine student eligibility for a grant. Such information may be required regarding parent/guardian's salary information provided for such purposes.	Article 6 (Contract/Legal Obligation)
Financial Payment Guarantee Letters	Collected from some international students for the purpose of invoicing their embassy.	Article 6 (Contract/Legal Obligation)
CCTV images	Collected only as per CCTV Policy	Article 6 (Legitimate interests)
Video images incl identifiable individuals	Not routinely collected by the Registrar's Office, but may be collected for assessments in some modules.	Article 6 (Legitimate interests)
Voice recordings	Not routinely collected but may be collected as part of assessments.	Article 6 (Legitimate interests)
Clinical files re research participants	Not routinely collected from students. If data is collected from students, it is subject to ethical scrutiny by Marino Ethics in Research Committee.	Article 6 (Contract/Legal Obligation)
Research subject consent forms	Not routinely collected, but student details are submitted to studentsurvey.ie for invitation to participate in this national survey (covered by a Data Sharing Agreement). Other research consent is subject to separate consideration by Marino Ethics in Research Committee.	Article 6 (Contract/Legal Obligation)

Appendix 2 - Processing of Special Categories of Personal Data

Categories of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, and which merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms of an individual. When processing special categories of data (see Section 6.11, sensitive data), it is necessary for the processing to be covered both by a legal basis under GDPR Article 6 GDPR Article 6(*Lawfulness of processing*) and by a special category condition set out under GDPR Article 9 (*Processing of Special Categories of Personal Data*). MIE must satisfy one of the GDPR Article 9 conditions listed below before processing sensitive data.

Sensitive Data
Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade-union membership
The processing of genetic data for the purpose of uniquely identifying a data subject
The processing of biometric data for the purpose of uniquely identifying a data subject
Data concerning health
Data concerning a data subject's sex life or sexual orientation

GDPR Article 9 **Conditions for Processing Sensitive Data**
An individual has given explicit consent to the processing of their sensitive data for one or more specified purposes

The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the individual in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the individual;
The processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent;
The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individual(s);
The processing relates to personal data which are manifestly made public by the individual;
The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the individual;
The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards;
The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of individuals, in particular professional secrecy; and

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the individual.