National Museum of Ireland

Data Protection Policy

Date Approved: 10/6/2021	Approved By: NMI Board
Implementation Date: June 2021	Lead Responsibility: Corporate Affairs Manager
Document Number: 2	Version Number: 3
Number of Pages: 15	Review Date: 2022

Contents

1. Purpose

The purpose of this Data Protection Policy is to outline the National Museum of Ireland ("NMI") policy in relation to the safeguarding of the rights and freedoms of data subjects when processing their personal data. NMI is committed to protecting the rights and privacy of individuals in accordance with both European Union and Irish data protection legislation. NMI shall lawfully and fairly process personal data about employees, suppliers, stakeholders and other individuals to achieve its mission and functions.

Data protection laws confer rights on data subjects as well as responsibilities of the parties processing personal data. This policy sets out how NMI has a responsibility to protect personal data and ensure its confidentiality, integrity and availability. To ensure compliance, NMI is required to put in place appropriate organisational and technical measures to prevent unauthorised internal and external access to personal data.

2. Definitions

The following table identifies some of the terms referred to within this policy.

Term	Definition
Data Controller	The Controller is responsible for the processing and is 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.
Data Processor	Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Officer	A National Museum of Ireland appointed officer with responsibility for the Data Protection compliance of the organisation.
Data Subject	A data subject is any identified or identifiable natural person, whose personal data is processed by the controller responsible for the processing.
GDPR	The EU General Data Protection Regulation (GDPR) - Regulation 2016/679 which came into effect in May 2018 and replaced the Data Protection Directive 95/46/EC and the Irish Data Protection Act(s).
Personal Data	Personal data means 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, CCTV footage, 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.
Processing	Processing is 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,

Term	Definition
	structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive Personal Data	Any personal data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.
Profiling	Profiling means 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 person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	Pseudonymisation is 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.
Recipient	Recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
Third Party	Third party is 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.
Consent	Is where the data subject provides freely given consent, 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. This legal basis applies in limited circumstances where a data subject has a genuine free choice and is able to withdraw the consent without suffering any detriment.

3. Scope

This policy applies to all of NMI's personal data processing functions in relation to identified or identifiable natural persons, including those performed on employees, suppliers and any other personal data NMI processes from any source.

For the purposes of this policy "employees" stands for all persons employed by NMI on a full or part time basis, persons who NMI contracts for services on a seasonal or ongoing basis, trainees with NMI, interns with NMI and agency employees.

4. Principles

There are a number of **important principles** relating to personal data to which NMI adheres. These are:

1. Personal data should be processed lawfully, fairly and in a transparent manner ("**lawfulness**, **fairness and transparency**")
2. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("**purpose limitation**");
3. Personal data should be adequate, relevant and limited to what is necessary ("**data minimisation**");
4. Personal data should be accurate and, where necessary, kept up-to-date ("**accuracy**");
5. Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary ("**storage limitation**");
6. Appropriate technical and organisational security measures should be applied to personal data to protect against unauthorised or unlawful access and accidental loss, destruction or damage ("**integrity and confidentiality**").

NMI should be accountable for, and able to demonstrate, its compliance with applicable data protection laws ("**accountability**").

There may be some instances where NMI may restrict the scope of data protection obligations and rights (Article 23). Restrictions can only be applied, if approved by the Data Protection Officer.

A description of how each of these data protection principles is implemented in practice is set out in Section 5 below.

5. Policy and Procedures

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation. NMI's policies and procedures are designed to ensure compliance with the following principles:

5.1 Personal Data must be processed lawfully, fairly and transparently

Lawfully: The legal basis for processing personal data is broadly based on Article 6.1(c) or 6.1(e) of the GDPR i.e. 'necessary for compliance with a legal obligation' or 'necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller'. NMI may also process personal data in accordance with certain contracts it has put in place and, in limited circumstances, where it has a legitimate interest in processing personal data. In very limited circumstances, NMI may request the consent of the data subject to process their data. In such cases, consent will be sought at the time that the data is collected, and the data subject will be advised that they can withdraw their consent at any stage during processing.

Fairly: For processing to be fair, NMI has to make certain information available to data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently: NMI provides the required information to data subjects at the time personal data is collected. NMI ensures that the information provided is detailed and specific, and that such notices are understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. In order to balance the requirements above, NMI may implement appropriate policies to make information available on its websites, forms or booklets. The information provided must include information about personal data collected both directly from the data subject and from other sources.

5.2 Personal Data can only be collected for specific, explicit and legitimate purposes

NMI collects and processes personal data only for the purposes for which it is collected. NMI employees must be alert to requests for processing of personal data for purposes for which it was not collected; no matter how related the processing may appear. Processing should only continue after an assessment of the impact of the new processing has taken place. This assessment may be done as a data protection impact assessment, please see section 6.6 of this policy.

5.3 Personal Data must be adequate, relevant and limited to what is necessary for processing

NMI ensures that in designing methods of data collection, whether online, forms or at its offices, that only the personal data required to identify the data subject(s) and provide the product or service requested is processed. NMI undertakes regular reviews of the data requested to ensure that the amount of personal data collected is minimised.

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

All data subjects have a right to ensure that their data is accurate and complete. NMI needs accurate and up-to-date data about data subjects to ensure that the correct services are

provided. All data collection procedures should be designed to ensure that reasonable steps are taken to update personal data where new data has been provided. All changes to personal data should be shared with each third party with whom the previous data had been shared, unless this is impossible or requires disproportionate effort.

5.5 Personal Data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing

NMI implements appropriate policies and procedures to ensure that personal data is retained only for the minimum period required to provide the services requested. This may be done by destroying the personal data, by anonymisation or any other appropriate method.

5.6 Personal Data must be processed in a manner that ensures appropriate security

NMI implements appropriate technical and organisational measures to ensure that appropriate security of the processing of personal data is applied.

5.7 Accountability for demonstrating compliance

NMI ensures that it maintains adequate records of its processing and evidence that it has complied with this policy and related policies and procedures. Responsibility for collecting and maintaining the evidence is with the Data Protection Officer. See section 6 of this policy for further guidance.

5.8 Rights of individuals whose data is collected

NMI designs and maintains appropriate policies, procedures and training to implement the following data rights of data subjects.

5.8.1 Right to access

Data subjects have the right to access their personal data. They are entitled to receive a copy of their data held by NMI and other information about the processing of the personal data. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

NMI implements procedures to ensure that requests from data subjects for access to their personal data are identified and fulfilled in accordance with the legislation within the 30 days permitted. For a copy of the Subject Access Policy, please contact the Data Protection Officer.

5.8.2 Right to information

Data subjects have the right to obtain confirmation from NMI whether their personal data is being processed.

5.8.3 Right to rectification

Data subjects have a right to have their personal data rectified where it is inaccurate or incomplete.

NMI is committed to holding accurate data about data subjects and implements processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

5.8.4 Right to erasure

Data subjects have a right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'.

Where NMI receives requests from data subjects looking to exercise their right of erasure then NMI will carry out an assessment of whether the data can be erased. In some instances, the right to erasure does not apply where NMI is required to:

- perform a task carried out in the public interest;
- retain the personal data for the establishment, exercise or defence of legal claims; or
- retain the personal data for archiving purposes.

Where the right to erasure can be implemented, then this will be done. Please consult with the Data Protection Officer regarding erasure requests.

5.8.5 Right to restriction of processing

Data subjects have a right to block or suppress processing of their personal data in defined circumstances. When processing is restricted, NMI is permitted to store the personal data, but not further process it.

NMI implements and maintains appropriate procedures to assess whether a data subject's request to restrict the processing of their data can be fulfilled. Where the request for restriction of processing is carried out then NMI will write to the data subject to confirm the restriction has been implemented and when the restriction is lifted.

5.8.6 Right to data portability

Data subjects have a right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Where NMI has collected personal data on data subjects by consent or by contract then the data subjects have a right to receive the data in electronic format to give to another data controller. It is expected that this right will apply only to a small number of data subjects. NMI will implement appropriate procedures to transfer only the relevant personal data.

5.8.7 Right to object

Data subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority;
- direct marketing; and
- processing for purposes of scientific/historical research and statistics.

Data subjects have a right to object to the processing of his or her personal data. The processing must have been undertaken on the basis of public interest or legitimate interest of NMI. Where such legal bases exist then NMI implements and maintain procedures to allow data subjects to pursue their right to object.

5.8.8 Right to withdraw data protection consent

Data subjects have the right to withdraw their consent to the processing of their personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may at any time directly contact the Data Protection Officer or another employee of the controller.

5.8.9 Right to complain

NMI maintains a complaints process whereby data subjects are able to contact the Data Protection Officer. The Data Protection Officer will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject is informed of their right to bring their complaint to the Data Protection Commission and their contact details.

6. Policy Responsibility

This Policy is approved by NMI Board, maintained and updated by the Data Protection Officer in consultation with the NMI Data Governance Team. It is reviewed at least annually by the Data Protection Officer to ensure alignment to suitable risk management requirements and its continued relevance to current and planned operations, legal developments and/or legislative obligations.

All NMI employees are expected to be familiar with this policy and to adhere to it as well as to its applicable principles and other related procedures, arising from such principles and obligations. All NMI employees will receive awareness training as part of their induction please see 6.1.1 below.

Further comments or questions on the content of this policy should be directed to the Data Protection Officer. Any material changes to this policy will require approval by the Board.

6.1 Responsibilities of Employees and Related Parties

All employees and any related parties, who process personal data on behalf of NMI, share the responsibility for adhering, implementing and complying with this data protection policy.

6.1.1 Training

All employees will receive training on this policy. New joiners will receive awareness training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the law or our policy and procedures.

Training is delivered via online methods and covers:

- Relevant and applicable regulatory principles, responsibilities and obligations related to Data Protection.
- NMI's data protection and related policies and procedures.

Completion of data protection training is compulsory.

6.1.2 Failing to comply with this policy

NMI takes compliance with this policy very seriously. Failure to comply puts individuals and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our organisational procedures, which may result in dismissal.

6.2 Ensuring appropriate technical and organisational measures

NMI implements appropriate technical and organisational measures to ensure and be able to demonstrate that personal data is adequately protected.

6.3 Maintaining a record of processing

NMI maintains a record of its data processing activities in the manner prescribed by Regulation. The Record of Processing is reviewed on a quarterly basis by the Data Governance Team and signed off by the Data Protection Officer not less than on an annual basis.

6.4 Implementing appropriate agreements with third parties

NMI implements appropriate agreements, memoranda of understanding and contracts (collectively “agreements”) with all third parties with whom it shares personal data. All such agreements are implemented in writing prior to the commencement of the transfer of the data. The agreement specifies the purpose of the transfer, the requirement for adequate security, right to terminate processing, restricts further transfer to other parties, ensure that responses are given to requests for information and the right to audit.

For the purposes of this policy, the term Third Parties refer to any entity, whether a member of NMI or external to it, who processes personal data on behalf of NMI.

6.4.1.1 Transfers of Personal Data outside of the European Economic Area

NMI will not transfer the personal data of the data subject outside of the European Economic Area unless an adequate level of protection is ensured.

6.5 Data Protection by Design and by Default

Data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This helps to ensure better and more cost-effective protection for individual data privacy.

Data protection by default means that service settings are automatically data protection friendly. An example of this would be that new network folders would be accessible only to those that require access specific to their role.

NMI develops processes, prior to the time of determining the means of processing as well as when actually processing, to incorporate appropriate technical and organisational measures to implement the data protection principles set out in Section 4 and integrate necessary safeguards into the processing to meet GDPR requirements.

6.6 Data Protection Impact Assessments

NMI implements procedures and documentation whereby all new types of processing, in particular using new technologies, that could result in a high risk to the rights and freedoms of its data subjects must carry out a data protection impact assessment. As part of this process, a copy of the impact assessment must be shared with NMI’s Data Protection Officer.

Where NMI is unable to identify measures that mitigate the high risks identified then NMI will consult with the Data Protection Commission prior to the commencement of processing.

6.7 Personal Data Breaches

NMI defines a 'personal data breach' as meaning 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 (e.g. the most common breach incidents that can occur are correspondence issuing to an unauthorised third party). NMI deems any loss of personal data in any format to be a personal data breach.

In the event of a suspected data breach, NMI employees must notify the Data Protection Officer immediately. In accordance with the GDPR, the Data Protection Officer will notify the Data Protection Commission without undue delay where a breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved.

The Data Protection Officer will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the Data Protection Officer will arrange for the data subjects to be notified.

NMI has put in place organisational and technical measures to prevent personal data breaches; these measures include checking procedures, security and employees training and awareness. For a copy of the Data Breach Policy, please contact the Data Protection Officer.

6.8 Appointment of the Data Protection Officer

NMI is required under GDPR to appoint a mandatory Data Protection Officer.

The appointment of a person to the role of Data Protection Officer and any supporting employees is based on a number of criteria, including:

1. Experience and knowledge held by the person to carry out the responsibilities of the role in a reasonable manner;

2. Adequate time to fulfil the requirements of the role; and

3. Sufficient seniority within the organisation to carry out the role.

6.8.1 Responsibilities of the Data Protection Officer

The Data Protection Officer will be responsible for *the following duties:*

- Provide advice and information to NMI employees and its processors on all aspects of Data Protection law and its effects on NMI 's processes and procedures;
- Monitor compliance with GDPR and all associated NMI policies and procedures by NMI employees and any external processors, through a defined and auditable risk-based monitoring plan;
- Where requested/ required by the circumstances, to provide advice to NMI on the outcome of a Data Protection Impact Assessment carried out within the Business;
- Co-operate with the Data Protection Commission, and any other Supervisory Authority which may have cause to contact NMI, and to act as the single point of contact with NMI for issues in relation to the processing of personal data by NMI;
- Be accessible to all data subjects of NMI with regard to the rights of data subjects over their personal data;

- Carry out all of their responsibilities with the appropriate level of confidentiality as required by the circumstances in which they are carrying out their role; and
- Provide regular reporting to the Board of NMI.

6.9 Governance

NMI monitors ongoing compliance with EU and Irish data protection laws through the Data Protection Committee. The Data Governance Team:

- Determines metrics for monitoring and reporting key data protection statistics;
- Receives regular reports from the Data Protection Officer;
- Reviews data protection impact assessments and approves or not the design of data protection elements of projects;
- Instigates investigations of data protection matters of interest, where and when applicable;
- Arranges internal audits, or similar, of NMI units for compliance with this policy, and other such activities relating to NMI's compliance with EU and Irish Law in the area of data protection.

7. Retention Periods

Further to point 5.5 above - NMI should not retain personal data longer than is required by law, contract or any other legal or contractual obligation. Personal Data is retained in accordance with the established guidelines within NMI's Retention Policy.

8. Related Documents

Policy, Procedure or Other Document Name	Policy Link	Policy Owner
Retention Policy		
Subject Access Request Policy		
Data Breach Policy		
Privacy Notice		
NMI Archives Policy		

Appendix 1

Revision Table

Version	*Primary Author(s)*	*Description of Version*	*Date Completed*
1.0			
2.0			
3.0			
4.0			
5.0			