NORTHERN IRELAND HUMAN RIGHTS COMMISSION

NIHRC Data Protection Policy and Procedures

Version No:	1 (c)
Version Issue Date:	10 September 2025
Supersedes Version:	*1 (b)*
Approved by	Director (Finance, Personnel and Corporate Affairs)
Created Date	April 2024
Last Review	August 2025
Next Review	August 2026
Plan Owner	NIHRC

Version Control	Date and details of change
Version 1	Approved by Director (Finance, Personnel and Corporate Affairs)
Reviewed April 2023	April 2023 – amends made to include missing Appendix 4 – complying with a Subject Access Request
Version 1 (a)	Appendix 4 added.
Reviewed April 2024	April 2024 – amend made to remove reference to Appendix 5 as not required.
Version 1 (b)	Reference to Appendix 5 removed.
Reviewed August 2025	August 2025 – amended to reflect changes in privacy notice
Version 1 (c)	Privacy notice updated to reflect amends

Northern Ireland Human Rights Commission Data Protection Policy and Procedures

Foreword

This policy and supporting procedures will inform Northern Ireland Human Rights Commission (NIHRC) employees and Commissioners about the key data protection issues, including General Data Protection Regulation (GDPR). It sets out information needed to ensure that the NIHRC complies with its data obligations and reference further guidance should that be necessary.

This policy and supporting procedures aim to ensure that all staff, stakeholders and third parties are aware of both their Data Protection rights and responsibilities including those arising from GDPR and to minimise the risk to the NIHRC of any Data Protection potential breaches.

All staff have a part to play in managing personal information safely, so are required to read this policy. The Data Protection Officer is also available to provide further advice to ensure that NIHRC complies with the GDPR.

Thank you.

1. The Northern Ireland Human Rights Commission Data Protection Policy

Statement of Policy

The NIHRC (the NIHRC) is fully committed to ensuring personal data is managed in accordance with the provisions of the General Data Protection Regulation (GDPR).

This policy relates to all personal data held by the the NIHRC. The types of personal data that NIHRC may be required to handle include information about

- Past and present employees;
- Past and present Commissioners;
- Employees of funded groups;
- Suppliers;
- Others we work with, advise or support.

All personal data, held by the NIHRC, whether as computerised records or as manual filing systems, is subject to the safeguards set out in the GDPR. This policy sets out how the NIHRC will process that personal information to enable it to perform its functions in accordance with the GDPR.

Privacy by Design, Data Minimisation and Pseudonymisation are key to the NIHRC's approach to data protection. In order to demonstrate best practice and compliance with the GDPR, the ICO advises that privacy and data protection is a key consideration in the early stages of policy development and then throughout its lifecycle. Adhering to the concepts of Privacy by Design, Data Minimisation and Pseudonymisation will help the NIHRC comply with its obligations under legislation.

Policy Awareness

All employees will be made aware of the NIHRC's Data Protection Policy Statement and Procedure by their line managers, and are expected to read and understand this policy and if they require clarification contact the Data Protection Officer for advice. This policy will be made available in written format, electronic format and published on our website.

This policy applies to all employees of the NIHRC, whether permanent or temporary workers, casual staff, agency staff and volunteers when working in for the NIHRC. It also includes the Commissioners when acting in that capacity.

All managers and employees have responsibilities for complying with the requirements of the GDPR by ensuring they process personal data in line with the data protection principles set out in Section 4.

Responsibilities

The Chief Executive, as the Accounting Officer, has overall responsibility for the Data Protection Policy. The Director (Finance, Personnel and Corporate Affairs) in the role of the Data Protection Officer is responsible for developing and enforcing information and records management practices. The Audit and Risk Management Committee provides oversight on behalf of the Board.

Changes to the Policy

The NIHRC reserves the right to change this policy at any time.

2. Background

The GDPR aims to protect privacy and prevent data breaches. Personal data means any information that relates to an identifiable living person. It may include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion or sexuality.

It can also include an individual's email address or job title if that sufficiently picks them out so they can be identified (in isolation or with other information held). The above is not exhaustive and any information that relates to an individual can be personal data.

The GDPR gives protection for personal data and imposes obligations on those who process personal data.

Controllers and Processors

- "Data controller" is defined as a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.
- "Data processor", in relation to personal data, is defined as a person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.
- "Processing", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. What this means is that even storing and holding information is categorised as "processing" under the GDPR. Both Data Controllers and Data Processors carry out Processing.

The definition of 'processing' suggests that a data processor's activities must be limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure. Activities such as interpretation, the exercise of professional judgement or significant decision – making in relation to personal data must be carried out by a data controller.

In most present cases where the NIHRC processes personal information, the NIHRC will be the Controller.

The GDPR provides the following rights for individuals:

1. The right to be informed.
2. The right of access.
3. The right to rectification.

4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

The NIHRC develops its policies and procedures to ensure that the above rights granted to individuals by GDPR are protected.

3. Data Protection Principles

The GDPR is underpinned by a set of six data protection principles that require personal data to be processed in such a way as to embed the concept of privacy by design.

1. Lawful, fair and transparent

There has to be legitimate grounds for collecting the data and it must not have a negative effect on the data subject or be used in a way they wouldn't expect.

2. Limited for its purpose

Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.

3. Adequate and necessary

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected. NIHRC will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

4. Accurate and up to date

Reasonable steps must be taken to keep the information up to date and change it if it is inaccurate.

5. Not kept longer than needed

Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.

6. Integrity and Security

Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction and kept safe and secure.

4. Data Security and Risk Management

The NIHRC will process all personal data it holds in accordance with its Information Security Policy.

The NIHRC is the data controller for the data it requests and processes from the data subjects. Sometimes the NIHRC asks other organisations to process the data on its behalf; these organisations are the data processors for the NIHRC.

Data Privacy Impact Assessment (DPIA)

Data Privacy Impact Assessments (DPIA's) are an integral part of how the NIHRC delivers Privacy by Design, Data Minimisation and Anonymization, together with other GDPR obligations are embedded in the NIHRC's approach to policy and procedure development.

Data protection risk is unique in that the NIHRC must manage its own corporate risk as well as risk to the data subjects. DPIAs are a tool that is used to identify and mitigate privacy risks of projects as well as corporate risk. DPIAs can help design more efficient and effective processes for handling personal data and thus reduce the risk to the NIHRC as an organisation and the data subject.

Conducting a DPIA is the most effective way to demonstrate that personal data processing complies with the GDPR. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used, where this is possible and devising more straightforward processes for staff.

A DPIA must be completed before beginning a new project, drafting a new or revising an existing procedure or policy, when preparing a business case or issuing an invitation to tender. Each DPIA must be reviewed and approved by the DPO before progressing the associated work any further. Should expenditure expected to be less than £5k but will involve personal data, the project must be reviewed and approved by the DPO, who may make relevant recommendations.

The NIHRC's Data Privacy Impact Assessments template is included in Appendix 6.

An Overview of Data Privacy Risk

Examples of Data Protection risks to the NIHRC and the Data Subject are

Risk	Data Subject	NIHRC
Financial Loss	X	
Financial Penalties		X
Loss of personal data	X	X
Breach of legislation		X
Loss of Reputation	X	X
Incorrect decision based on inaccurate data	X	

Examples of where control weakness that fail to mitigate data privacy risk include:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about;
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Key considerations in designing privacy into the NIHRC's procedures that determine the appropriate approach to minimising risk include:

- Deciding not to collect or store particular types of information;
- Ensuring information is minimised and held in the appropriate format;
- Ensure procedures require personal data to be anonymised wherever possible;
- Applying to date retention schedules;
- Ensuring staff are properly trained and are aware of potential privacy risks;
- Ensuring the appropriate legal basis for processing is applied and data subjects are suitably informed; and
- Ensuring GDPR compliance third party agreements are in place.

5. Lawful Basis for Processing

The Lawful Basis for processing personal information must be determined before processing can begin. At least one of the following must apply:

Consent	The individual has given clear consent for you to process their personal data for a specific purpose.
Contract	The processing is necessary for a contract you have with the individual or because they have asked you to take specific steps before entering into a contract.
Legal Obligation	The processing is necessary for you to comply with the law (not including contractual obligations).
Vital Interests	The processing is necessary to protect someone's life.
Public task	The processing is necessary for you to perform a task in the public interest or for your official functions and the task or function has a clear basis in law.
Legitimate interests	The processing is necessary for your legitimate interests of a third party unless there is a good reason to protect

the individual's personal data which overrides those legitimate interests.

It is important to get this right first time. If the NIHRC finds at a later date that its chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

Factors to consider include:

- What is the NIHRC's purpose in processing this information
- What is the NIHRC trying to achieve
- Can the NIHRC reasonably achieve it in a different way
- Does the NIHRC have a choice over whether or not to process the data

The NIHRC was established as a result of the Belfast (Good Friday) Agreement. Our governing legislation is the Northern Ireland Act 1998, as amended by the Justice and Security (Northern Ireland) Act 2007 and the European Union (Withdrawal Agreement) Act 2020. It is a National Human Rights Institution with A status accreditation from the United Nations. This recognition means that the organisation operates independently in full accordance with the United Nations General Assembly Resolution 48/134 (the Paris Principles).

The NIHRC is also a non-departmental public body for the purposes of Section 75 (Equality Legislation), the Freedom of Information Act, has an Accounting Officer, is subject to managing Public Money and has a Framework Document in place with the Northern Ireland Office. Therefore, this policy places the NIHRC within the definition under Article 6(1) of a Public Authority. The NIHRC will apply the Public Task lawful basis whenever it is appropriate to do so.

Correspondingly it would be inappropriate for the NIHRC to use legitimate interest as the lawful basis and will not do so.

The lawful basis for processing and the basis for assigning that basis is documented by the Data Protection Officer and approved by the Chief Executive. The record of the lawful basis will be updated by the Data Protection Officer as required but will be reviewed at least once per year.

6. Right to be informed

The NIHRC will provide privacy information to individuals including:

- The purposes for processing their personal data;
- Retention periods for that personal data and
- Who the NIHRC will share the data with.

Where possible this will be provided at the point of collection. Where the NIHRC obtains personal data from other sources, such as grant claims, the NIHRC will

make arrangements to provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

The NIHRC will maintain a Privacy Notice on its website which will contain, as a minimum, the information shown in the table below and will be reviewed annually.

Name and contact details	The categories of personal data obtained
The contact details of the DPO	The recipients or categories of recipients of the personal data
The purposes of the processing	The details of transfers of the personal data to any third parties
The source of the personal data	The rights available to individuals in respect of the processing
The lawful basis for processing	The retention periods for the personal data
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	The details of the existence of automated decision-making including profiling

When the NIHRC collects personal data it will provide a copy of its privacy statement at the time, or in advance of obtaining the data. When the NIHRC obtains data from a source other than the individual it relates to, the NIHRC will arrange for the individual to be provided with the privacy information. The table below summarises how privacy information will be communicated to the NIHRC's main group of data subjects.

NIHRC employees	Through employee contracts and agreements
Newsletter recipients	Link to Privacy Notice on newsletter
Consultations	Link to Privacy Notice on consultations
Other Communications	Link to Privacy Notice on emails

7. Data Protection Officer

The GDPR introduces a duty for the NIHRC to appoint a Data Protection Officer (DPO) for public authorities. The role of the DPO is to assist the NIHRC to monitor internal compliance, inform and advise on the NIHRC's data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced and report to the highest management level. The DPO's tasks are defined in Article 39 and in ICO guidance as being:

- To inform and advise employees about obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR, other data protection laws and internal data protection policies;
- To advise on and to monitor data protection and impact assessments;
- Be the first point of contact for supervisory authorities and for individuals whose data is processed and
- To take into account the risk associated with processing information the NIHRC is undertaking. The DPO must have regard to the nature, scope, context and purposes of the processing.

Where those charged with governance decide not to follow the advice given by the DPO, they should document their reasons to help demonstrate accountability.

It is assumed that the roles and responsibilities of the DPO will sit in the office of the Director (Finance, Personnel and Corporate Affairs). The NIHRC recognises that the Director (Finance, Personnel and Corporate Affairs) is also the Data Controller, creating conflict of interest with their role as DPO. Given the size of the NIHRC there is no way for the organisation to avoid this risk while assigning the role of DPO to a post with sufficient competencies and access to carry out the function. As a mitigating control the DPO will log and report all data protection events and report these to the Chief Executive and Audit and Risk Management Committee. This log will be available for internal audit review.

8. Disclosure and Sharing of Personal Information

The NIHRC sometimes needs to share information with other organisations, for example if:

- It is under a duty to disclose or share a data subject's personal data in order to comply with any legal or regulatory requirements;
- To enforce or apply any contract with the data subject or other agreements with whom the data subjects have an agreement; or
- To protect rights, property, or safety of staff, board members, stakeholders, suppliers or others (including those it works with, advises or supports).

Any third parties who are users of personal information supplied by the NIHRC will be required to confirm and demonstrate they will abide by the requirements of the GDPR. This will be evidenced by use of a Third Party Processing Agreement. Audits may be carried out at any time by NIHRC to ensure compliance.

Where a third party is processing data on behalf of the NIHRC, the third party will be a Data Processor and therefore a third party agreement will be required. That agreement will identify the following in relation to data processing:

- The subject matter and duration of the processing;

- The nature and purpose of the processing;
- The type of personal data and categories of data subject and
- The obligations and rights of the controller.

The third party agreement will include the following requirements from the processor:

- To only act on the written instructions of the controller;
- To ensure that people processing the data are subject to a duty of confidence;
- To take appropriate measures to ensure the security of processing;
- To only engage sub-processors with the prior consent of the controller and under a written contract;
- To assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- To assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- To delete or return all personal data to the controller as requested at the end of the contract; and
- To submit to audits and inspections, provide the controller with whatever information it needs to ensure they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

In certain circumstance, information relating to employees acting in a business capacity may be made available provided:

- We have the statutory power or are required by law to do so; or
- The information is clearly not intrusive in nature; or
- The employee has consented to the disclosure; or
- The information is in a form that does not identify individual employees.

The ICO have provided checklists for 'systematic data sharing' and 'one-off requests' in their Data Sharing Code of Practice, which are particularly helpful when starting a new project or programme which may involve sharing of personal data.

A sample third party processing agreement and third party confidentiality agreement are attached as appendices to this policy.

Confidentiality must be respected, where appropriate. Employees within the NIHRC should not disclose personal information to any third party unless they believe it is fair and lawful to do so.

9. Retention of Data

The NIHRC holds different types of information for different lengths of time, depending on the legal and operational requirements. The NIHRC will keep some forms of information longer than others in line with financial, legal or archival requirements.
The NIHRC maintains a Data Retention and Disposal policy with supporting procedures that provide a list of retention periods and provides guidance on maintenance of the NIHRC's Information Asset Register. Information will not be held for any longer than is needed and personal information will be clearly identified.

10. Subject Access Request

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Individuals will have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The NIHRC will provide a copy of the information free of charge. However the NIHRC will charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

The information will be provided without delay and at the latest within one month of receipt. If the request is complex or numerous the NIHRC will extend the period of compliance by a further two months and will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The NIHRC will verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, you should provide the information in a commonly used electronic format.

Detailed guidance on complying with a Subject Access Request is set out in Appendix 4.

11. Providing Access to Individual Rights

As noted under Section 3, the GDPR gives data subjects' eight specific rights to their personal data. The GDPR introduces the obligation from organisations to

have procedures in place to ensure that those rights can be exercised on request. The Right to Access is considered under Section 10: Subject Access Request above. The remaining seven rights are considered below.

Right to Rectification

The GDPR gives individuals the right to have inaccurate personal data rectified and to have incomplete personal data completed. Even when the NIHRC have implemented effective internal control to ensure accuracy and completeness of personal data, the GDPR creates the obligation for the data controller to consider accuracy upon request.

Right to Erasure

The NIHRC will erase personal data of individuals where the following conditions are met:

- The personal data is no longer necessary for the purpose originally collected or processed;
- Where consent is the lawful basis for holding the data, and the individual withdraws that consent;
- Processing the personal data for direct marketing (e-newsletter) purposes and the individual objects to that processing;
- The NIHRC has processed the personal data unlawfully;
- You have to do it to comply with a legal obligation.

Right to Restrict Processing

The NIHRC will restrict processing of personal data of individuals where one of the following conditions are met:

- The individual contests the accuracy of their personal data while the NIHRC is verifying the accuracy of the data;
- The data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- The NIHRC no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim.

As there are close links between the Right to Erasure, the Right to Restrict and the Right to Object, the NIHRC, as matter of good practice, will automatically restrict the processing whilst it is considering the accuracy or the legitimate grounds for processing the personal data in question.

The NIHRC will consider the following steps when complying with a request to restrict processing:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from the distribution lists.

The NIHRC will not process the restricted data in any way except to store it unless:

- The NIHRC has the individual's consent;
- It is for the establishment, exercise or defence of legal claims;
- It is for the protection of the rights of another person (natural or legal) or
- It is for reasons of important public interest.

Right to Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or their performance of a contract and
- When processing is carried out by automated means.

Right to Object

The right to object affords individuals the right to object to:

- Processing based on 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.

When an objection is received where personal data is processed due to a public task, the NIHRC will stop processing the personal data unless the DPO can demonstrate:

- Compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- Of the processing is for the establishment, exercise or defence of legal claims.

Where the NIHRC processes personal information for the performance of a public task it will inform individuals of their right to object "at the point of first communication" and in its privacy notice.

When an objection is received where the lawful basis is consent, such as the e-newsletter, the NIHRC will interpret this as consent being withdrawn and cease to process immediately. There are no exemptions or grounds to refuse.

Rights related to automated decision-making including profiling

At present the NIHRC does not make automated decisions. Should this change the NIHRC will update its procedures accordingly.

Complying with a request to exercise Individual Rights

On receipt of a request the NIHRC will take all reasonable steps to ensure that the data subject's rights are exercised. What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important the right is, the personal data and the data subject, the greater the effort the NIHRC will make delivering that individuals right.

The GDPR allows an individual to make a request to exercise their rights in writing and to any part of, or person, within the NIHRC. Furthermore a request to exercise their rights does not need to mention the right being exercised. For example, if an individual has challenged the accuracy of their data and has asked for it to be corrected, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request. A record of all requests is maintained by the DPO.

All requests must be reported immediately to the Data Protection Officer. The DPO will prepare a plan within 72 hours detailing what steps the NIHRC will take to comply with the request. The NIHRC will comply within one calendar month of the request being received unless there are exceptional circumstances. Should exceptional circumstances exist, the data subject will be notified and a report made to the Audit and Risk Management Committee.

A fee cannot be charged.

The NIHRC will restrict processing of personal data during the period when the accuracy of personal data is being checked or updated.

The DPO will write to the individual once the extent of accuracy of personal data has been established and rectified.

In certain circumstances the NIHRC can refuse to comply with a request to correct personal data. Should these circumstances apply, the DPO will report to the Chief Executive explaining why they apply and what action should now be taken. The decision not to comply must be approved by the Chief Executive and reported to the Audit and Risk Management Committee.

12. Data Breach

A data breach is defined by GDPR as "any unauthorised or unlawful processing, accidental loss or destruction of, or any damage to, personal information held by the NIHRC in both electronic and paper copy".

Data breach incidents should be reported to the DPO verbally by the NIHRC employee who becomes aware of the data breach as soon as the data loss has been discovered. A formal breach report form (as shown in Appendix 3) should then be immediately completed by the NIHRC employee who becomes aware of the data breach. The completed form should be forwarded to the DPO without delay.

Such incidents will be reported to the Information Commissioner's Office within 72 hours and to the data subject as soon as possible.

How to respond to a data breach

Whilst breaches should be escalated immediately (even if all the details are not yet clear), it is important that staff also bring any 'near miss' incidents or information security weaknesses to the attention of their line manager. If you become aware that data security has been breached, you must inform your line manager immediately. The line manager in turn, must advise the DPO who will assess the severity of the incident and notify the Chief Executive. The Chief Executive and DPO will together agree a way forward.

The DPO must report the breach to the ICO within 72 hours of the NIHRC becoming aware of the breach and also inform the data subject without delay.

The DPO will present a report on the incident including:

- Summary of the event and circumstances;
- Type and amount of personal data affected;
- Actions taken by recipient who received the information;
- Actions taken to retrieve the information and respond to the breach;
- Procedures in place to mitigate risk and why not effective;
- Details of notification to affect data subject(s);
- Has a complaint been received from a Data Subject
- Assessment of risk to data subject and the NIHRC with proposed mitigating actions;
- Details of communication with the ICO;
- Proposed changes to procedure to reduce risks of repeat and
- Reporting and other recommendations.

This report will be presented to the Chief Executive as soon as possible and no more than 10 working days from the date of the incident and a summary report will be provided to the Audit and Risk Management Committee. Should an Audit and Risk Management Committee meeting take place before the report is complete the Committee should be briefed on the incident at the earliest opportunity.

The DPO will also update the ICO on the progress of the report and the conclusions and procedure and policy changes identified to reduce the risk of a repeat data security breach.

The breach will be notified to the Northern Ireland Office and formally reported through the quarterly assurance statement.

In the event of a near miss, the DPO should initiate an investigation in order to ensure weaknesses are addressed and lessons learned are disseminated. The DPO will set a timeframe for an investigation to allow him/her to provide a short report to the Chief Executive within fifteen working days. The Chief Executive

and the DPO will then together agree a way forward and decide on whether or not there is an operational need to report the near miss as per the steps outlined above.

13. The Role of the Information Commissioner's Office

The Information Commissioner's Office (ICO) has a range of statutory powers to assess and enforce compliance with the GDPR. The main powers are outlined briefly below.

ICO Register of Data Controllers

The Information Commissioner maintains a public register of data controllers who process personal information. Each register entry includes the name and address of the data controller and a general description of the type of processing carried out. Notification is the process by which a data controller's details are added to the register. Anyone can consult the register to find out what processing is being carried out by a particular organisation.

The GDPR requires the NIHRC to notify the Information Commissioner's Office (ICO) on an annual basis. Prior to the expiry of the registration, the Data Protection Officer will request all business areas to closely examine the NIHRC's current notification details and advise of any additions or amendments required for the coming year.

Managers must ensure the purposes and purpose descriptions set out in the NIHRC's notification fully cover all the processing of personal information taking place within their business area. The DPO must be fully informed immediately if any new type of personal information is to be processed, or if a type of personal information is no longer to be processed. This will allow the NIHRC's notification to be amended as required by data protection legislation.

Failure to amend a record within 28 days of discovering the need for a change is a criminal offence so it is vital that all areas carry out this exercise every year and that our registration details with the ICO are kept up to date.

The NIHRC's entry number on the Information Commissioner's Data Protection Register is Z8970270 and can be viewed online.

Appendix 1 Glossary of Terms

Definitions

The following definitions are used in this policy and shall mean the following:

Consent	The individual has given clear consent for you to process their personal data for a specific purpose
The NIHRC	Northern Ireland Human Rights Commission
Data	Is information which is stored electronically on a computer or in certain paper-based filing systems
Data concerning Health	Any personal data relating to the physical or mental health of an individual or the provision of health services to them
Data Controllers	Are the people who or organisations which determine the purposes for which, and the manner in which any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. NIHRC is the data controller of the personal data used in the NIHRC
Data Erasure	Also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase further dissemination of the data and potentially have third parties cease processing of the data
Data Portability	The requirement for data controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller and allows for the transfer of the personal data to that other data controller
DPIA	Data Privacy Impact Assessment, a process which enables organisations such as NIHRC to identify and reduce the privacy risks of any particular project. Also known as a PIA.
Data Processors	Includes any person or organisation that is not a data user that processes personal data on NIHRC's behalf and on its instructions. Staff of data controllers are excluded from this definition but it could include suppliers which handle personal data on NIHRC's behalf, for example companies who store our information backups
Data Protection Authority	National authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the European Union. Also known as a Supervisory Authority
Data Protection Officer	An expert on data privacy who works independently to ensure that an entity is adhering to the policies

	and procedures needed to be compliant with the GDPR. Also known as DPO.
DSA	Data Sharing Agreement- agreement between two or more parties for the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation
Data Subject	A natural person whose personal data is processed either by a data processor or a data controller
Data Users	Are those staff whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and the Security Policies
Encrypted Data	Personal data that is protected through technological measures to ensure the data is only accessible/ readable by those with specified access
Filing System	Any means of categorising data that makes it accessible according to specific criteria, or able to be queried
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
PECR	Privacy and Electronic Communications Regulations 2003
Personal Data	Means data relating to a living individual who can be identified from that data (or from that data and other information in its possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes
Privacy by Design	A Principle that calls for the inclusion of data protection principles from the onset of the designing of systems, rather than as an addition at a later stage
Processing	Is any activity that involves use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using =, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties
Profiling	Any automated processing of personal data without the input of a person, intended to evaluate, analyse or predict the behaviour of a data subject

Pseudonymisation	The processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure that it cannot be attributed to the data subject
Recipient	Entity to which personal data is disclosed
Right to be Forgotten	Also known as Data Erasure, it entitles the data subject to have the data controller erase his or her personal data, cease further dissemination of the data and have third parties cease processing of the data
Right to Access	Also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a data controller has concerning them
SAR	Subject Access Request- request from an individual to see their own data under the rights given to them in the GDPR
Supervisory Authority	A public authority established by a member state of the European Union in accordance with Article 46 of the GDPR, which is tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations with the European Union
Special Category Data	Includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the NIHRC of, or proceedings for any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Appendix 2 Privacy Notice: General Data Protection Regulation

Data Controller Name: Northern Ireland Human Rights Commission
Address: 4th Floor, Alfred House, 19-21 Alfred Street, Belfast, BT2 8ED
Telephone: +44(0)2890 243987
Email: info@nihrc.org
Data Protection Officer: Director (Finance, Personnel and Corporate Affairs)
Telephone: +44(0)2890 243987
Email: info@nihrc.org

Purpose of data purpose of data processing and legal basis for processing

Communication purposes

The NIHRC retains contact details for individuals (such as email addresses and telephone numbers) with consent for the purpose of a public task to fulfil its statutory function to promote awareness of human rights through education, training and research under section 69(6) of the Northern Ireland Act 1998.

Legal function

Where a person seeks assistance from the NIHRC in relation to proceedings involving law or practice and the protection of human rights which a person in Northern Ireland has commenced, or wishes to commence; or proceedings in the course of which such a person relies, or wishes to rely, on such law or practice the NIHRC, under section 70(3) of the Northern Ireland Act 1998 Act may (a)provide, or arrange for the provision of, legal advice; (b)arrange for the provision of legal representation; (c)provide any other assistance which it thinks appropriate.

To assist in fulfilling this public task the NIHRC retains and processes personal data received through legal enquiries (i.e. received by telephone, through its legal clinic, through receipt of case file). This work is often conducted in private and the information obtained may be confidential. Assistance provided by the NIHRC may be subject to professional privilege. Details may be shared regarding legal casework by the NIHRC, including an application for assistance, with third parties (i.e. an organisation with which the NIHRC has a Memorandum of Understanding, the courts, legal counsel). Sharing of personal information with third parties will normally be done with consent, unless the NIHRC is otherwise required to do so (i.e. legislation, contract, public task, vital interests.)

Investigations

The NIHRC for the purpose of an investigation under section 69 of the Northern Ireland Act 1998 Act may, by notice in writing require a person to provide information, to produce documents in his possession, or to give oral evidence. The NIHRC may require a person to provide information in public and publish the details of the information, documents, or evidence in order to fulfil this public task.

By virtue of the 1998 Act section 8A, the NIHRC shall publish a report of its findings on an investigation. Where the NIHRC receives information or documents from or relating to an intelligence service in response to a notice under section 69A(1) of the 1998 Act, the NIHRC shall store and use the information or documents in accordance with any arrangements specified by the Secretary of State.

Contracts

The NIHRC retains contact and bank details for its contractors as required by law and may share this information with its sponsor department, the Northern Ireland Office, and the National Audit Office in accordance with rights of access requirements.

Personnel

The NIHRC processes personal information of its employees in accordance with the law for the proper carrying out of its functions as an employer.

In relation to applicants for employment the NIHRC will use the personal information they supply to process the application and to monitor recruitment statistics. If as part of this process, the NIHRC intends to disclose information to a third party such as taking up a reference or obtaining a disclosure certificate from Access NI, the NIHRC will not do so without first informing the applicants beforehand unless the disclosure is required by law. Personal information about unsuccessful applicants will be destroyed.

The NIHRC keeps a personnel file in respect of each employee which will be used for purposes directly relevant to that person's employment.

Transfer of personal data to other countries

Sometimes it may be necessary for the NIHRC to transfer personal information overseas (i.e. the European Court of Human Rights or the United Nations). Any transfers made will be in full compliance with all aspects of the General Data Protection Regulation.

How long will personal data be retained

The NIHRC will only retain personal data for as long as necessary and in line with our Retention and Disposal Schedule.

Communication purposes

Personal information held by the NIHRC to fulfil its statutory function to promote awareness of human rights through education, training and research is retained with the consent of individuals and is reviewed once a year. The NIHRC contacts everyone for whom it retains information for this purpose and asks if they wish

to remain on the NIHRC's contacts database. If, at any time, an individual wishes to withdraw their consent without detriment they can do so by emailing or by writing to the NIHRC.

Legal function

Personal information held by the NIHRC to fulfil its legal function is retained as follows:

Litigation files are retained for 7 years following closure to ensure legal and/or financial obligations are met.

Applications for assistance by an individual are retained for 7 years (particularly in those cases where the NIHRC decides to hold a watching brief on litigation).

Enquiries are retained for 1 year following closure.

Investigations

Personal information held by the NIHRC for the purpose of an investigation is retained for one year following the publication a report of its findings, unless the NIHRC is otherwise required to do so (i.e. legislation, contract, public task, vital interests).

Contracts

The NIHRC retains contact details for its contractors and other information relevant for the duration of a contract for six years plus a further year following the completion of the contract as required by the statutory retention period.

Personnel

The NIHRC retains personnel records (including disciplinary records) for a period of six years after employment ceases as a recommended (non-statutory) retention period.

The retention of other relevant personnel records is included in the NIHRC's data retention and disposal policy.

Special categories of personal data

The NIHRC retains personal information as an employer required by legislation for the following special categories:

- race;
- ethnicity;
- community background;
- age;
- gender;
- trade union membership;
- disability;

- health;
- marital status;
- number of dependents and children;
- sexual orientation.

Organisations that we share information with

The NIHRC share information with the following organisations

Criminal Justice Inspection Northern Ireland;
Community Relations Council;
Commission for Victims and Survivors for Northern Ireland;
Commissioner for Older People for Northern Ireland;
Equality Commission Northern Ireland;
Regulation and Quality Improvement Authority;
National Audit Office;
Northern Ireland Commissioner for Children and Young People;
Northern Ireland Office;
Northern Ireland Public Services Ombudsman;
Police Ombudsman for Northern Ireland;
Prisoner Ombudsman for Northern Ireland;

Sharing of personal information with third parties will normally be done with consent, unless the NIHRC is otherwise required to do so (i.e. legislation, contract, public task, vital interests.)

The NIHRC may share your data with criminal justice and relevant enforcement agencies for the prevention or detection of crime.

What rights do I have?

The General Data Protection Regulation provides the following rights for individuals https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/:

1. You have the right to obtain confirmation that your data is being processed, and access to your personal data;
2. You are entitled to have personal data rectified if it is inaccurate or incomplete;
3. You have a right to have personal data erased and to prevent processing, in specific circumstances;
4. You have the right to 'block' or suppress processing of personal data, in specific circumstances;
5. You have the right to data portability, in specific circumstances
6. You have the right to object to the processing, in specific circumstances;
7. You have rights in relation to automated decision making and profiling.

Visitors to our website

When someone visits our website, we collect internet log information and details of visitor behaviour patterns. We do this to monitor the number of visitors to the various parts of the site but collect this information in a way which does not identify anyone.

When we want to collect personally identifiable information through our website, we will be up front about this (for example, website forms). We will make it clear when we collect personal information and we will explain what we intend to do with it.

Use of cookies

The NIHRC will not use cookies to collect personably identifiable information about you. However, if you wish to restrict or block the cookies which are set by the NIHRC's website, or indeed any other website, you can do this through your browser settings. The Help function within your browser should tell you how.

The NIHRC uses Google Analytics, a web analytics service provided by Google, Inc. Google Analytics sets cookies on the NIHRC's website on its behalf in order to compile reports for us on user activity and how visitors use our site.

The cookies collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited. This is used to help us improve the website. More information is available online from Google.

Google may transfer this information to third parties where required to do so by law or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google.

If you would like more information about the cookies used by Google Analytics, please see their individual privacy policy. You can also opt out of being tracked by Google Analytics.

The NIHRC's Cookie Policy can be found at https://nihrc.org/cookie-policy

Cookies set by Third Party Sites

When you visit a page with content embedded from, for example, Facebook, YouTube or Twitter, you may be presented with cookies from these websites. The NIHRC does not control the dissemination of these cookies. You should check the relevant third party website for more information about these and we would urge you to review these, as they will govern the use of information you submit or which is collected by cookies whilst visiting these websites.

- Facebook
- Twitter

- You Tube

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit www.allaboutcookies.org

How do I complain if I am not happy?

If you are unhappy with how any aspect of this privacy notice, or how your personal information is being processed, please contact the *NIHRC's Data Protection Officer at:*

Northern Ireland Human Rights Commission
4th Floor, Alfred House
19-21 Alfred Street
Belfast
BT2 8ED

Tel: +44 (0) 28 9024 3987

Email: info@nihrc.org

http://www.nihrc.org/

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Email: casework@ico.org.uk
https://ico.org.uk/global/contact-us/

Appendix 3. The Northern Ireland Human Rights Commission

Breach of Data Security Report Form
Staff Report

Name .....

Position .....

Email Address .....

a) When did you first become aware of the incident?

b) Provide a description of the incident

c) How did you become aware of the incident?

d) Confirm the incident has been reported to your line manager

e) Supporting Documents – Please attach any supporting documentation

Signed .....

Date .....

When completed this form should be returned to the Director (Finance, Personnel and Corporate Affairs) in the capacity of the Data Protection Officer, by emailing info@nihrc.org

Or by post to:

Director (Finance, Personnel and Corporate Affairs)
Northern Ireland Human Rights Commission
4th Floor, Alfred House
19-21 Alfred Street
Belfast
BT2 8ED

Appendix 4. The Northern Ireland Human Rights Commission

Complying with a Subject Access Request

To comply with Subject Access Requests, the NIHRC has the following checklist in place:

- Respond to a subject access request without undue delay and within one month of receipt. This can be extended by a further two months if the request is complex or the NIHRC has received a number of requests from the individual, eg other types of requests relating to individuals' rights.

- Understand how to perform a reasonable search for the information. The NIHRC should make reasonable efforts to find and retrieve the requested information. However, the NIHRC is not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

- Understand what we need to consider if a third party makes a request on behalf of an individual. The NIHRC needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

- Are aware of the circumstances in which the NIHRC can extend the time limit to respond to a request. The NIHRC can extend by a further two months if the request is complex or the NIHRC has received a number of requests from the individual, eg other types of requests relating to individuals' rights.

- Understand how to assess whether a child is mature enough to understand their rights. The NIHRC will respond directly to the child if it is confident that the child can understand their rights. The NIHRC may allow the parent or guardian to exercise the child's rights on their behalf if the child authorises it, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make the request on their behalf.

- Understand that there is a particular emphasis on using clear and plain language if the NIHRC is disclosing information to a child.

- Understand that the NIHRC needs to consider if a request includes information about others. The NIHRC should understand whether it is possible to comply with the request without disclosing information that identifies another individual. If this is not possible, the NIHRC does not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent. The NIHRC will respond to the requester whether or not it decides to disclose information about a third party. The NIHRC must be able to justify the decision to disclose or

withhold information about a third party, and a record will be kept of what has been decided and why.

- The NIHRC is able to deliver the information securely to an individual, and in the correct format. The method in which the NIHRC provides the information to the individual will, in part, be guided by any request they have made about what format they would like to receive it. If the NIHRC has any concerns over the method that the individual has requested to be used, it will contact them, explain the concerns and ask for an alternative address or method of providing the information. If this is not possible, and the information is being provided electronically, consideration will be given to providing it in an encrypted form, followed by a password being shared separately. The NIHRC notes that this depends on the nature and sensitivity of the information. The NIHRC may also consider delivery by post and consideration will be given to special delivery or courier service, depending on the nature and sensitivity of the information.