Housing Executive

Response to:
FOI_22-23_197
January 2023

GDPR Policy

1. **Could you email me a copy of your GPDR policy.**

   Below is a copy of NIHE's GDPR policy.

Housing Executive

DATE: 29 MAY 2019

POLICY AND PROCEDURES FOR HANDLING PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION ACT 2018

DATA PROTECTION

Policy Title:	Policy and Procedures for Handling Personal data under the General Data Protection Regulation and Data Protection Act 2018
Author(s):	David Mayers, DPO
Ownership:	Data Protection Team Policy applies to all Housing Executive Staff
Date Created:	13 August 2018
Approved by:	Board
Date Approved:	29 August 2018
Operational Date:	27 September 2018
Review Timeline:	Every 3 years or as required
Review Date:	29 May 2019
Next Review Date:	01 September 2021
Version Control:	Version 1.2
Replaces:	Procedures for Handling Personal Information under the Data Protection Act 1998
Explanation for Review:	The Housing Executive's Data Protection Policy was reviewed and updated to reflect recommendations outlined in the February 2019 audit.
Links to other NIHE Policies:	Disposal of Records Schedule
Key Words:	Data Protection; GDPR; Data Subject Rights (DSR); Subject Access Requests (SAR); Personal Information; Data Protection Officer (DPO); Information Commissioner's Office (ICO); Sharing Personal Information; Lawful Basis.

Version Record

Version No	Amendments Made	Authorisation
V1	N/A – Original Document	Board – 29/08/18
V1.1	Version Control Record included in document	DPO – 01/04/19
V1.2	• Inclusion of a formal procedure for closing and archiving DSRs in cases where the individual does not validate their request by providing identification; • Inclusion of who may approve the release of data for departments in the absence of a Level 9 officer; • Inclusion of archiving procedure for closed requests.	DPO – 29/05/19

Contents

1.0 Scope

The aim of the Policy and Procedures outlined in this document is to ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. This policy applies to all staff undertaking duties on behalf of the Housing Executive and applies to personal data in any form; written, photographic or verbal.

2.0 Data Protection Policy Statement

2.1 Introduction

The Housing Executive is committed to carrying out its statutory functions and its role as an employer in a manner which respects and protects the privacy of an individual.

The Housing Executive collects, uses and retains information about our customers and stakeholders in our role as a data controller. We also receive general information and personal data about other individuals in the course of those dealings. These individuals are collectively called 'data subjects' and include Housing Executive staff, applicants for housing and renovation grants etc.

'Personal data' can be factual information, such as name and address, or expressions of opinion about or intentions towards individuals. It can occur in any format, for example, word documents, databases, spreadsheets, emails, CCTV, index cards, paper files and verbally i.e. during an interview or telephone call with a customer.

The policy applies throughout the life of the data, from collection to destruction or passed to PRONI for permanent preservation.

2.2 General Data Protection Regulation (GDPR)

GDPR (Regulation (EU) 2016/679) is applicable to all member states of the European Union (EU) since 25 May 2018. GDPR places a greater emphasis on accountability and being able to demonstrate that there are procedures in place to protect the personal data rights of all data subjects.

The DPA 2018 updates the UK data protection law and applies GDPR standards in domestic law. The DPA 2018 makes provision for how GDPR applies in the UK and covers additional areas outside GDPR such as law enforcement and immigration.

The Housing Executive's compliance with these data protection laws will be monitored by the Data Protection Officer (DPO) and supported by this policy.

2.3 Purpose

The purpose of this policy is to provide a framework to enable the Housing Executive to:

a. Comply with GDPR and the DPA 2018 regarding personal data;
b. Protect the rights of Housing Executive customers, service users, staff and other individuals;
c. Protect the organisation and its officers from the consequences of a breach of its responsibilities;
d. Follow good practice.

2.4 The Housing Executive's Commitment to Data Protection

The Housing Executive is committed to compliance GDPR and the DPA 2018. We treat this responsibility as a fundamental obligation and one that is in keeping with our role as the strategic housing authority for Northern Ireland.

As such, we endorse the data protection principles outlined in section 5.0 and expect our staff to take reasonable steps to ensure compliance with the data protection legislation and in particular to adhere to our data protection procedures as set out in this policy.

2.5 Contact

For data protection queries:

Data Protection Officer,
Legal Services,
Housing Centre,
2 Adelaide Street,
Belfast, BT2 8PB.

Email: dataprotection@nihe.gov.uk

Information Commissioner's Office (ICO) website: www.ico.org.uk.

2.6 Resources

Additional resources mentioned throughout this policy are available on the GDPR Gateway page.

3.0 Governance: Roles and Responsibilities

3.1 Board, Chief Executive and the Directors

The Board has overall responsibility for information governance, including data protection. The Chief Executive is responsible for assuring that all risks to data

protection and information security are effectively managed with overall responsibility for the management, review and implementation of this policy. Each Director has responsibility for ensuring and assuring compliance with this policy and the data protection laws within their functional areas.

3.2 Data Protection Officer

GDPR introduced a requirement for public bodies to appoint a Data Protection Officer (DPO) to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding privacy by design and act as a point of contact for data subjects and the Information Commissioner's Office (ICO).

In accordance with GDPR the DPO remains independent at all times. This means the DPO cannot be instructed or directed as to "what result should be achieved, how to investigate a complaint or whether to consult the regulatory authority".

The task of the DPO to monitor the organisation's compliance with GDPR does not make the DPO individually liable for non-compliance by the organisation. The guidance from Europe states that organisations are free to ignore the advice of DPOs as they remain "responsible for compliance", but when doing so must document in writing the reasons for not following the advice. The DPO reports directly to the Chief Executive on matters arising out of his role.

The Data Protection Officer's duties include:

a. Overall responsibility for ensuring that information threats and data security breaches are identified assessed and any personal data breaches managed;
b. Informing the ICO of notifiable breaches within 72 hours of the organisation becoming aware of the breach;
c. Providing information and advice to the organisation and its employees about their obligations to comply with data protection legislation;
d. Providing advice (where requested) regarding Data Protection Impact Assessments (DPIAs) and monitor performance;
e. Monitoring compliance with data protection legislation;
f. Acting as a point of contact for and cooperating with the ICO;
g. Monitoring prompt and appropriate responses to Data Subject Requests (DSRs);
h. Maintaining and renewing the Housing Executive's registration with the ICO ensuring that it accurately reflects its data processing activities.

The Housing Executive is legally obliged to demonstrate its compliance with GDPR. The DPO will therefore report all data protection activity on a quarterly basis to the Audit and Risk Assurance Committee (ARAC).

3.3 Information Asset Owners

Assistant Directors have been appointed as Information Asset Owners (IAOs) and are listed in the corporate structure which can be found under the People & Organisation tab of Gateway.

IAOs are responsible for ensuring that information assets 'owned' by their functional areas are managed in line with this policy and relevant legislation.

The IAOs role has been expanded to facilitate compliance. Previously Assistant Directors were assigned as IAOs to electronic systems; this role now extends to include hard copy data i.e. paper files, both open or retained. Whilst this role has been designated to all level 9 post holders, the IAO may allocate associated activities to a nominated officer or officers to ensure compliance with GDPR and the DPA 2018.

The role of an IAO within their area(s) of responsibility is to:

a. Ensure awareness and application of Data Protection Policy and Procedures;
b. Ensure application of the Retention and Disposal Schedule;
c. Ensure that all information assets are identified and the DPO is advised of any changes needed to ensure that the Information Asset Register is kept up to date;
d. Ensure staff awareness and compliance with the breach notification procedure as outlined in section 13.0;
e. Ensure a Data Protection Impact Assessment (DPIA) as outlined in section 6.8 is undertaken if there are changes to current projects or new processing requirements involving personal data;
f. Ensure compliance with data security and the organisation's policies on clear desks, password security, encryption and security for removal of personal data for out-of-office working as outlined in section 8.0;
g. Ensure all forms used to collect personal data are updated and include a reference to the organisation's Privacy Notice and are clear regarding the collection and use of personal data;
h. Ensure all staff have completed GDPR e-learning for the first time and annually thereafter.

IAOs should liaise with the DPO if specific data protection guidance is required for their business functions. This may include specific operational procedures or training to ensure that data protection practice is established and followed.

3.4 Data Subject Request Co-ordinators

Officers who undertake the Data Subject Request co-ordinator (DSR co-ordinator) role, previously known as the Subject Access Request (SAR) co-ordinator role, are responsible for processing DSRs relating to any of the enhanced data rights.

3.5 Managers

All managers are required to ensure that they (and their staff) are aware of, understand and adhere to this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated of any changes made to this policy. All managers must ensure that their staff undertake the data protection e-learning training and any training in information security which is specific to their role. Refresher training for all staff must be undertaken annually. Managers are responsible for ensuring that appropriate actions are taken following receipt of advice from the DPO.

3.6 All Staff

Staff (both contracted employees and agency workers) must be aware of, understand and adhere to this policy. All staff have a responsibility for data protection and are required to complete any associated training and confirm their acceptance of the Housing Executive's IT Security Policy before accessing any systems containing personal data.

All staff must:

a. Understand the main concepts of data protection legislation, the six GDPR principles, special category data and the need for lawful bases for processing personal data;
b. Be aware of and know the applicable lawful bases for processing personal data within their area of work;
c. Identify and report any risks to the security of personal data processed by the Housing Executive to the DPO or to their Line Manager (who will notify the DPO and the relevant IAO);
d. Assist customers to understand their rights and the Housing Executive's responsibilities regarding data protection;
e. Identify and forward any Data Subject Requests (DSRs) to dataprotection@nihe.gov.uk . DPO to monitor DSRs in accordance with the process set out in this policy.

3.7 Information Commissioner

The Information Commissioner is an independent official who reports directly to Parliament.

3.8 Information Commissioner's Office

The Information Commissioner's Office (ICO) is an independent authority in the UK that promotes openness of official information and protection of private information. The ICO does this by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action against breaches of data protection legislation.

The ICO oversees:

a. The Data Protection Act (DPA) 2018;
b. The Freedom of Information Act 2000;
c. The Environmental Information Regulations 2004;
d. The Privacy and Electronic Communications Regulations 2003;
e. The General Data Protection Regulation (GDPR).

The ICO can exercise the following regulatory powers:

a. Enforcement Notice
   Notice served by the Information Commissioner to compel a data controller to take a specific course of action in relation to the processing of data.

b. Assessment Notice
   This relates to the powers for the ICO to conduct a compulsory audit.

c. Information Notice
   This is a requirement from ICO to provide information for an investigation.

d. Monetary penalty
   The ICO can impose monetary penalties up to 4% of annual turnover or £17m, whichever is greater.

4.0 Definitions

4.1 Personal data

Personal data is anything that identifies or relates to a living person either by itself or when put together with other information.

This includes:

a. The names and other details of tenants, grant applicants, housing benefit claimants, housing applicants, homelessness applicants, employees, and other individuals with whom we do business;
b. The names and other details of those who correspond with us or provide details during telephone calls;

c. Information about contractors and suppliers of goods and services;
d. Information held by managers about their staff, such as performance management information;
e. Word processed documents, spreadsheets and databases which contain personal details such as names and addresses;
f. Emails, where either the person sending or receiving is identifiable or the contents refer to identifiable people.

Collectively this personal information is known as 'personal data'. The information is generally held in computer systems such as HMS, I-world (Housing Benefit), Payroll and PSMS (Grants), Outlook mailboxes and a range of other local specific databases 'owned' by Departments.

4.2 Data Subject

The data subject is the person to which the personal data relates. This includes Housing Executive customers, their partners, dependants and Housing Executive staff. All references to the data subject should be understood to mean the data subject or their legal representative.

4.3 Special Category Data

Special category data under GDPR and the DPA 2018 is broadly similar to sensitive personal data under the Data Protection Act (DPA) 1998. It is personal data which is considered more sensitive and needs further protection. In particular, this type of data could create significant risks to a person's fundamental rights and freedoms, for example, by putting a person at risk of unlawful discrimination. See section 6.2 for more detailed information.

Examples of special category data include information about an individual's:

a. Race or ethnic origin;
b. Political opinions;
c. Religious beliefs or other beliefs of a similar nature;
d. Trade union membership;
e. Physical or mental health;
f. Sex life or sexual orientation.

Note: Personal data relating to criminal convictions or related security measures is processed by other provisions outside special category data.

4.4 Data Controller

The data controller determines the purposes, conditions and means of the processing of personal data. The Housing Executive is a data controller in most

instances. However, circumstances could arise where the Housing Executive may also be a data processor.

4.5 Joint Data Controller

Where two or more controllers jointly determine the purposes, conditions and means of processing.

4.6 Data Processor

A data processor processes personal data on behalf of the data controller, for example:

a. Companies or contractors who carry out maintenance and improvement contracts;
b. Belfast City Council who process data on behalf of the Housing Executive for Housing Benefit purposes.

A list of who we share information with is available via the following link:
Who we share data with
This is not an exhaustive list and may be subject to change.

4.7 Processing (In relation to personal data)

Processing is defined as collecting, recording or holding personal data or performing any operation or set of operations on personal data, including:

a. Accessing or viewing data;
b. Organisation, adaptation or alteration of the data;
c. Retrieval, consultation or use of the data;
d. Disclosure of the data by transmission, dissemination or otherwise making available;
e. Alignment, combination, blocking, erasure or destruction of the data.

4.8 Filing system

This is any structured or unstructured set of personal data which is accessible according to specific criteria.

4.9 Redaction

The removal of data that is exempt from disclosure by whatever means is required, for example, electronic redaction or using a redaction pen on both sides of the paper on a photocopy of the original document. The original document must not be altered in any way.

4.10 Exempt data

Certain data, which can be legally withheld when responding to a DSR and which relates to:

a. National security, defence, public security;
b. Prevention, investigation, detection or prosecution of a criminal offence;
c. Public interest, economic or financial interests.

Any queries regarding GDPR Derogations or DPA 2018 Exemptions should be referred to the DPO for advice.

5.0 GDPR Principles

The Housing Executive must follow the six GDPR principles when processing personal data i.e. when it is being collected, used and stored. The law demands that compliance with those principles can be demonstrated. This is key to the Housing Executive being able to demonstrate accountability for the processing of personal data. It is therefore essential that all processing of personal data complies with the six GDPR principles listed below:

5.1 Lawfulness, fairness and transparency

Personal data should be processed lawfully, fairly and in a transparent manner in relation to individuals.

This requires openness and honesty in all processing activities. It is important to be transparent when acquiring personal data from people. Individuals have the legal right to be informed about the collection and use of their data. This is done through the organisation's Privacy Notice. See section 6.1 on Lawful Basis for further information.

5.2 Purpose

Personal data should be collected for specified and legitimate purposes and not further processed outside the intended purpose.

5.3 Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purpose.

When collecting personal data the purpose for which it is to be used should be clear and only personal data necessary to achieve that purpose should be collected. A record of that decision should be kept. Do not collect irrelevant information simply because it might be useful at some point in the future. Consider whether pseudonymised or anonymised information would achieve the same result as information with a name attached.

5.4 Accuracy

Personal data should be accurate and where necessary, kept up to date. Reasonable steps should be taken to ensure that inaccurate personal data is rectified without delay.

When creating file notes, comments about individuals should be based on recorded facts and defensible as accurate if challenged. Whenever writing anything about individuals, it is important to be professional. Individuals have a right to ask to see what is written about them.

5.5 Storage

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data has been processed. Records must be disposed of in line with the Housing Executive's Disposal of Records Schedule.

Personal data may be stored for longer periods where it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Staff should ensure that this data is safeguarded in line with this policy and IT Security.

5.6 Security

Appropriate measures should be put in place to protect the confidentiality and integrity of personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

6.0 Collecting personal data

Personal data obtained, created and held by Housing Executive staff as a result of their work are part of our corporate records. These records are subject to the procedures and business rules governing the management of records outlined in our Records Management Handbook which can be found on the GDPR Gateway page.

6.1 Lawful basis

The first GDPR principle, that processing of personal data must be lawful, requires the Housing Executive to ensure that processing is being carried out on a lawful basis. If the processing is unlawful an individual will have the right to have that data erased. GDPR and the DPA 2018 set out the six lawful bases for processing which are summarised below:

Consent	The individual has freely given clear consent to process their personal data for a specified purpose.
Contract	Processing is necessary for a contract with an individual.
Legal Obligation	Processing is necessary to comply with the law.
Vital Interests	Processing is necessary to protect someone's life
Public Task	Processing is necessary to perform a task in the public interest, for official functions and the task or function has a clear basis in law.
Legitimate Interests	Processing is necessary for legitimate interests unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Public Task or Legal Obligation may be used where processing is necessary to comply with relevant legislation. If either Public Task or Legal Obligation are not appropriate lawful bases, the other lawful bases should be considered.

When processing is necessary for the performance of any of the Housing Executive's statutory functions (which includes duties and powers) the appropriate lawful basis is considered Public Task. If the processing can be linked to any of the Housing Executive's statutory functions, then it can be reasonably assumed that the processing is justified on the grounds of Public Task. Where processing is necessary for the Housing Executive to comply with the law, the lawful basis of Legal Obligation may be appropriate. Where Public Task or Legal Obligation are the most appropriate lawful bases, consent should not be used.

As a public body the Housing Executive has limited scope to rely upon Legitimate Interest, which will not apply where Public Task is applicable. Legitimate Interest may apply to our role as an employer e.g. HR functions.

If a lawful basis cannot be established, the DPO should be contacted for advice before commencing processing.

6.2 Special Category data

To process special category data (previously known as sensitive data) at least one of the conditions below must be satisfied (GDPR Article 9(2)). When considering this it is important to understand that it does not have to be the same as that used for the lawful basis. For example, if consent is used as the lawful basis for processing, this does not restrict the choice of the condition for the special category processing to that of explicit consent.

The conditions are:

a. The data subject gives explicit consent to the processing;
b. It is necessary for the purposes of carrying out the obligations and exercising specific rights;
c. It is necessary to protect the vital interests of the data subject or of another natural person incapable of giving consent;
d. It is carried out in the course of its legitimate activities;
e. It relates to personal data which are manifestly made public by the data subject;
f. It is necessary for the establishment, exercise or defence of legal claims;
g. It is necessary for reasons of substantial public interest;
h. It is necessary for the purposes of preventive or occupational medicine;
i. It is necessary for reasons of public interest in the area of public health;
j. It is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical.

The condition used will depend on the purpose and reasons for processing the personal data. Advice should be sought from the DPO where there is any uncertainty regarding the appropriate condition for processing.

6.3 Consent

Consent is a freely given, specific and informed indication of the data subject's wishes, by which he or she signifies agreement to the processing of their personal data. Consent must be clear and concise and separate from the organisation's terms and conditions.

Consent should be used as a last resort where no other lawful basis for processing applies. To be valid, the consent must be freely given. If there is a clear imbalance of power between the controller requesting consent and the data subject, it is likely that the consent will not be valid. If an individual, dependent on any of our services could fear adverse consequences, they might feel they have no choice but to agree and as such, consent would not be considered to be freely given.

If consent is being considered as a lawful basis, please contact the DPO via dataprotection@nihe.gov.uk.

6.4 Withdrawing consent

Requests to withdraw consent including full details of the processing to which it relates must be sent to dataprotection@nihe.gov.uk or by post to:
DPO, 4th Floor, Legal Services, Housing Centre, 2 Adelaide Street, Belfast BT2 8PB.

The DPO will assess the request and advise staff on the actions to take with immediate effect. The requestor will be informed of the outcome using the template letters.

6.5 Privacy Notice

The Privacy Notice **must** be made available **at the point of data collection**.

The privacy notice informs people of:

a. Who is collecting personal data i.e. the identity of the controller, noted as 'The Housing Executive';
b. What data is being collected;
c. How it is being collected;
d. Why it is being collected;
e. How it will be used;
f. Who it will be shared with.

To comply with the transparency requirement it is vital that data subjects understand the content of the Privacy Notice at the point of data collection.

A copy of the organisations Privacy Notice can be found through the GDPR Gateway page or via the Housing Executive webpage via the following links:

NIHE Privacy Notice
NIHE Privacy Notice for Staff (HR)

6.6 Forms

The DPA 2018 outlines that the Privacy Notice must be easily understandable and in a prominent position to be seen. Please use the following format as a guide to ensuring forms are compliant with GDPR and the DPA 2018:

What we do with your information

You have applied to the Housing Executive to …….
The Housing Executive in processing your application is using the lawful basis of ……Public Task/Contract/ Legal Obligation, etc.
The Housing Executive requires the information to process your application to ……..
To find out more information about how we use your personal data and your personal data rights you can view the full version of our Privacy Notice at:
www.nihe.gov.uk/privacy_notice

Sharing your information with others

We will share your information with……..
Your information may also be shared with others for statistical analysis and fraud prevention/detection. Your information is only shared where this is necessary to comply with our legal obligations or as permitted by General Data Protection Regulation or Data Protection Act 2018.

Your Rights

Within certain limitations, you are entitled to view, request a copy, amend, delete, object to or restrict processing of your information.
We will retain your information in line with the Housing Executive's Retention Policy.

To discuss any aspect of making forms compliant please email dataprotection@nihe.gov.uk for further advice.

6.7 Data Protection by Design and by Default

Privacy and data protection are a key consideration in the early stages of any project and continues throughout the project's lifecycle. This enables the organisation to meet its legal obligations. For example, when:

a. Building new IT systems for storing or accessing personal data;
b. Developing policy or strategies that have privacy implications;
c. Embarking on a data sharing initiative; or
d. Using data for new purposes.

6.8 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) should be carried out when commencing a new project, specifically the implementation of new technologies, a change in processing activities or where the processing is likely to result in a high risk to an individual's data rights. The DPIA screening questions will determine if a DPIA is required.

Areas of high risk include, large scale processing of special category data or personal data in relation to criminal convictions or offences, profiling, decisions which have legal or significant effects on individuals and large scale monitoring of public areas (CCTV).

A DPIA includes the following:

a. Description of the processing operations and purposes;

b. Assessment of necessity and scale of the processing in relation to its purpose;
c. Assessment of risk to individuals;
d. Measures in place to address risk i.e. security and the need to demonstrate compliance and privacy solutions;
e. Sign off and record DPIA outcomes;
f. Integrate DPIA outcomes into project plan.

The DPO cannot complete a DPIA, but will be available in an advisory capacity for any business units considering a new project. The DPIA template is available on the GDPR Gateway page.

Templates should be completed and forwarded to dataprotection@nihe.gov.uk for review by the DPO.

This is a vital process as all changes must be reflected in the relevant Privacy Notice, Information Asset Register and Lawful Basis map.

6.9 Children

Under GDPR, where Information Society Services (most internet services but not preventative or counselling services) are offered directly to children and consent is the lawful basis, parental consent must be obtained. Under the DPA 2018 parental consent must be obtained for children under 13 years of age.

Housing Executive does not provide Information Society Services i.e. online services, to children.

The requirements concerning parental or guardian consent responsibilities could be relevant to third parties with whom personal data is shared but not in the context of preventative or counselling services.

7.0 Retention and Disposal of Personal Data

It is the responsibility of each member of staff to ensure that corporate records are managed in line with the Housing Executive's Disposal of Records Schedule.

7.1 Make retention/destruction decisions

As a general rule, unless documents are being retained as part of the corporate record, or there is a specific reason for keeping them they should be destroyed or deleted when they are no longer needed for the purpose for which they were obtained in line with the Housing Executive's Disposal of Records Schedule.

This includes electronic records and emails in personal drives or shared mailboxes, which should either be filed in the Housing Executive's Records Management

System or deleted. It is particularly important that emails containing special category data, for example information about someone's health, are not kept in mailboxes indefinitely.
Note: currently emails which are over 3 months old are deleted automatically.

If personal data is being kept for the corporate record, make sure it is included in the Disposal of Records Schedule agreed with the Records Manager and that it is destroyed in accordance with normal application of such schedules.

Guide to Implementing the Disposal Schedule
Disposal of Records Schedule

8.0 Keeping personal data secure

This section highlights key organisational guidance which aids compliance with the GDPR Article 5(f) principle on security.

8.1 User Security Policy

The User Security Policy defines the Housing Executive's policy for the security of its information assets and the Information Technology (IT) systems processing this information.

The Housing Executive's User Security Policy applies to:

a. All Housing Executive staff;
b. The staff and agents of other organisations (external to the Housing Executive) who directly or indirectly have been given permission to utilise Housing Executive IT systems or its information resources and have access to Housing Executive's IT Services or its information assets.

The Housing Executive Guide to Physical, Document and IT Security covers:

a. All Housing Executive information assets and supporting IT systems (including PCs) whether connected to a network or not;
b. The Housing Executive network itself;
c. All single and multiprocessing systems;
d. Third party services.

NIHE Guide to Physical, Document and IT Security

8.2 Store personal data securely

It is important that personal data is stored securely and access restricted to only those with a need or right to see it. This is particularly the case if special category data is involved, or sets of information about a number of people.

Care should be taken to ensure that personal data is not disclosed either verbally or in writing, whether accidentally or not, to any unauthorised third party and in particular, by taking the following measures:

a. Not leaving paper copies of personal data where anyone else can access them. Keeping manual personal records locked away securely;
b. Not leaving a computer unattended without locking it;
c. If the personal data is filed in the Housing Executive's Records Management System, setting access controls so that it can be accessed only by those with a need and a right to see it;
d. If the personal data is held outside the Housing Executive's Records Management System, using passwords to secure it.
e. Being mindful during discussion, interview, meeting or telephone call with a client not to tell them anything about another person unless there is a clear lawful basis for doing so.

8.3 Transmit personal data securely

Ensure that transmission of information, whether internally or externally, is done with a level of security appropriate to the nature of the information.

If the information is being transmitted within the Housing Executive by physical means, such as in an envelope, the envelope should be sealed and where possible the recipient alerted to the fact that it has been despatched. If it is being transmitted by email, ensure the email is marked with appropriate protective marking.

If special category data is being transmitted externally by electronic means e.g. to a contractor or other public body, the following rules apply:

a. Ensure the transmission has been approved by the IAO;
b. Use technical means such as encryption for transmission;
c. If a password is required, send it separately.

See the Housing Executive's Out of Office Security Policy for further guidance on the handling of personal data and other sensitive information when outside the office.

8.4 Retrieval of files from archive storage

Files held in archive storage containing personal data, or other business sensitive information, should be managed in a way that restricts access only to those individuals who are properly authorised to do so.

When requesting retrieval of files containing sensitive information, care should be taken to ensure that, once the files are delivered from storage, they are delivered promptly to the individual officer who made the request. If it is not possible to deliver them immediately (for example the requesting officer is out of the office), the files should be held in a secure area (e.g. locked cabinet, office or store room) until such time as they can be delivered to the appropriate officer.

The onus is, therefore, on the owner of the files (in this case the requestor) to ensure that appropriate arrangements are in place for the secure handling of the files from the point when they are delivered until they are returned to archive storage e.g. If the files contain personal data or special category data, they are delivered to a designated recipient.

8.5 Phone calls

Phone calls can lead to unauthorised use or disclosure of personal data, for example, by the caller pretending to be the data subject. The following precautions should be taken:

a. Staff must ensure they are confident of the caller's identity and their right to that personal data. If their identity cannot be satisfactorily confirmed, the personal data should not be disclosed ;
b. If a phone call requires authorised disclosure of personal data but in circumstances that would lead a member of the public to overhear, where practical alternative arrangements should be made, for example, moving to another location, to continue the phone call.

It should be noted that the above rules only apply to enquiries relating to personal data of a routine nature e.g. a tenant making enquiries about rent payments etc. All other requests for disclosure of personal data should be treated as DSRs and should be documented by staff in writing. If in doubt, advice should be sought from the DPO.

8.6 Destroy information securely

When deleting information held electronically, ensure that it is removed from the recycle bin. Destroy paper based personal data only under secure conditions either shred it or use a confidential waste bag. Further advice on this is available from the relevant Facilities Services Manager.

Further advice will be communicated regarding the deletion of records held on the Housing Executive's Records Management System and business function software systems.

8.7 Transfers Outside of the European Economic Area

The Housing Executive, except in response to a Subject Access Request (SAR), do not transfer personal data outside the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) unless (i) the data subject has given consent or (ii) a contract is in place which provides equivalent protection of the rights of data subjects.

8.8 Email

Emails, both incoming and outgoing, are covered by GDPR and the DPA 2018 if one or other of the following criteria is met:

a. the sender or recipient is identifiable, either through their email address or the text of the email;
b. The text of the email contains personal data, i.e. facts, opinions or intentions about identifiable living individuals.

Under the DPA 2018, emails in personal mailboxes (including deleted items), emails saved into the Housing Executive's Records Management System and emails placed on paper files that fall within the definition of a relevant filing system are liable for disclosure in response to a DSR. Copies of deleted emails held on back-up systems may also be liable for disclosure.

9.0 Sharing personal data with others

This section explains precautions to take if sharing personal data with another person or organisation.

Do not share personal data with anyone outside the Housing Executive without having first obtained approval from the relevant Assistant Director, Regional Manager or other Level 9 post holder, unless through existing approved data sharing arrangements.

If personal data is being passed to someone outside the Housing Executive, follow the guidance below and keep a record of the following:

a. Sufficient details of the information for it to be clearly identifiable subsequently;
b. The name of the person who has authorised it;
c. Details of whom it has been sent;
d. The date on which it was sent;
e. The means used to send it e.g. encrypted email.

The guidance above is suitable for situations where the information sharing relates to a single individual or small numbers of individuals in a one-off situation.

If considering sharing information on a larger scale, or smaller amounts of data but on a regular basis this process should generally be managed through a Data Sharing Agreement; the following section gives guidance in this area.

9.1 Data Sharing Agreements

A Data Sharing Agreement (DSA) provides a framework to ensure that the sharing of personal data between the Housing Executive and participating agencies, bodies, groups and organisations is compliant with GDPR principles. Business units considering entering into new data sharing arrangements and those currently sharing data should formalise such information sharing through a DSA unless there are sound reasons for not doing so, for example, the sharing is not of a recurring nature but a one off event.

IAOs must ensure that all DSAs are registered with the DPO who will maintain a central register. The IAOs must also ensure that the DPO is advised of any changes to the current provisions.

The need for a DSA will be included in the DPIA to be completed upon commencement of any relevant new projects.

Advice and guidance on setting up a new data sharing agreement can be sought from the DPO.

10.0 Data Subject Rights

GDPR provides increased rights for individuals. There are eight rights which are outlined below.
A copy of the data rights leaflet can also be found on the GDPR Gateway page.

10.1 Right to be Informed

Data subjects have the right to be informed of the collection and use of their personal data. This has been addressed through the 'Privacy Notice' (see Section 6.5) and 'Forms' (Section 6.6).

10.2 Right to Access

Individuals have the right to access their personal data and supplementary information. This is commonly known as a SAR. This right of access allows individuals to be aware of and verify the lawfulness of the processing.

10.3 Right to Rectification

GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Where action is not being taken in response to a request for rectification, the individual must be given a written explanation which must also inform them of their right to complain to the ICO and to a judicial remedy.

10.4 Right of Erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

This is not an absolute right nor is it limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

A request for erasure can be refused where the personal data is processed for the following reasons:

a. To exercise the right of freedom of expression and information;
b. To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
c. For public health purposes in the public interest;
d. Archiving purposes in the public interest, scientific research historical research or statistical purposes;
e. The exercise or defence of legal claims.

Where data has been shared for further processing, each recipient (i.e. a processor) must be contacted and informed of the erasure of the personal data unless this proves impossible or involves disproportionate effort. In this instance, individuals must be informed about these recipients.

10.5 Right to Restrict Processing

Individuals have a right to restrict processing of personal data. When processing is restricted, storage of the personal data is permitted but it is not to be processed any further. However, sufficient information should be retained about the individual to ensure that the restriction is respected in the future.

10.6 Right to Object to Processing

Individuals must be informed of their right to object 'at the point of first communication' which is outlined in the Housing Executive's Privacy Notice.

Individuals have the right to object to:

a. Processing based on legitimate interests or the performance of a task in the public interest or exercise of official authority (including profiling);

b. Direct marketing (including profiling);
c. Processing for purposes of scientific or historical research and statistics.

The objection must be on 'grounds relating to his or her particular situation'.

Processing must cease unless:

a. There are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual (which must be recorded);
b. The processing is for the establishment, exercise or defence of legal claims.

Upon receiving a request, further processing must be restricted whilst the objection request is under review. Where the objection request is upheld any further processing must be restricted.

10.7 Right to Appeal Automated Decision Making

Data subjects have the right to ask if automated decision making is taking place and to challenge that process. At present automated decision making only occurs through the Automated Transfer to Local Authority Systems (ATLAS) reports in Housing Benefit. The organisation has controls in place which ensure Housing Benefit staff review all automated decisions which can result in a retrospective change in the award of Housing Benefit. Claimants are informed of all decisions which result in a change to their Housing Benefit award. At present 20% of all automated decisions are reviewed by a member of staff.

10.8 Right to Data Portability

The right to data portability allows individuals 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.

This right only applies to the personal data an individual has provided to a controller where processing is based on consent, explicit consent or under a contract and by automated means. As the Housing Executive works primarily under the lawful basis of public task, this right is unlikely to be engaged.

At present the Housing Executive is unable to provide for data portability but will review this process through Data Protection by Design and Default processes in future.

11.0 Data Subject Requests

11.1 Requests

An individual (this includes members of staff) can make a DSR to **any member of staff either verbally or in writing**, including social media. The request should clearly indicate that it relates to an individual's own personal data, it does not have to include the following phrases to be considered as a DSR:

a. GDPR;
b. Data Protection Act 2018;
c. Subject Access Request;
d. Data Subject Request.

Where a request has been made verbally or via social media (this includes requests by staff members), staff should record the details of the request on the DSR form and complete the 'for Housing Executive use only' box. Staff should check with the requestor that they have understood their request, as this can help avoid later disputes about how you have interpreted the request. The request should be scanned and forwarded to dataprotection@nihe.gov.uk.

Where a requestor has highlighted an accessibility issue, staff should note the accessibility issue so that the response can be delivered to the requestor in a suitable form, if possible. DSR co-ordinators should contact the Equality Unit to ensure that further communication will be in a suitable format to accommodate the requestor through the Communication Support Policy.

A data subject may request any or all of the following:

a. Manual records;
b. Information held on computer including email;
c. Taped conversations or their transcripts;
d. Still photographs;
e. Any other media;
f. Request for data held on Close Circuit Television (CCTV) or audiotape.

Should a data subject request data from either CCTV or taped conversations; seek advice from the administrator of the CCTV system (usually the local office manager where the CCTV is sited).

A copy of the request should be scanned and emailed to dataprotection@nihe.gov.uk .

11.2 Requests from members of staff or ex-employees

Members of staff or ex-employees of the Housing Executive have the same rights under GDPR as members of the general public and data can be held on them both in their capacity as employees and as customers of the Housing Executive.

DSRs from staff or ex-employees requesting personnel details should be forwarded to dataprotection@nihe.gov.uk.

11.3 Confirming identity

The Housing Executive as a data controller is only obliged to respond to a request where the data subject supplies sufficient information to enable identification of the:

a. Person making the request;
b. Information requested.

Access will normally only be given to:

a. The data subject;
b. Someone authorised by the data subject (in writing) to receive the data;
c. An elected representative who is acting on behalf of the data subject.

It is the responsibility of the DSR co-ordinator (or the business unit receiving the request) to establish the identity of the person making a DSR. This is necessary to prevent an unauthorised disclosure of personal data.

Where a request is made by email, it is particularly important to establish the identity of the person making the request. Such information can, if considered appropriate, be obtained by telephone, so long as whatever questions are asked would provide sufficient confirmation.

Where an individual does not validate their request by providing evidence of their identity within 1 month of their initial request, the request will be closed and archived by the Data Protection Team on the DSR database. If an individual contacts the Housing Executive with their identification after their request has been closed, a new DSR request will be required and should be recorded as a new record on the DSR database.

11.4 Data subject representatives

A data subject can nominate a representative to act on their behalf. Disclosure of personal data to a representative should only be made where the consent of the data subject has been given, unless the representative is legally empowered to act on behalf of the data subject or is an elected representative (e.g. MP, MLA councillor or MEP) in their authorised capacity or role.

If there is any doubt about whether the representative is who they say they are, or whether consent is valid, data should not be disclosed. In all cases a decision must be made on an individual basis.

There are certain representatives who are legally empowered to act on behalf of a data subject, for example, a person given Power of Attorney (by a court or by the data subject themselves) deals with all aspects of the data subject's affairs. If this is the case, staff should request a copy of the relevant documentation or available evidence so that they may disclose any data to that representative that could normally be given to the data subject.

Data cannot be disclosed to someone just because they work for a representative group such as the Citizen's Advice Bureau (CAB) or welfare rights groups unless the customer has consented. A written form of authority or consent must be provided prior to release of personal data.

Before disclosing data to anyone other than the data subject, staff must be satisfied that the representative is:

a. Who they say they are;
b. Either acting with the consent of the data subject or has been appointed by a government department or a court to act for the data subject.

11.5 Elected Representatives

Elected representatives include MP's, MLA's, MEP's and Councillors. An elected representative or a person acting with their authority (e.g. an MP's personal assistant) may contact the Housing Executive to request personal data on behalf of an individual. Requests for information from elected representatives are usually routine queries regarding repairs, housing applications etc. If the disclosure of personal data, including special category data is considered relevant and necessary regarding such a request, the Housing Executive can disclose personal data to respond to the request without insisting upon evidence such as the individual's consent or formal assurance from the elected representative that that is the case.

If there is doubt about whether the personal data to be disclosed in response to the request is relevant and/or necessary or it is not a routine query, consent may be required from the individual or further evidence from the elected representative to provide the Housing Executive with a lawful basis for disclosing the personal data.

Where requests involve personal data relating to criminal convictions and offences, additional conditions need to be met for disclosure (GDPR Article 10). The DPO should be contacted for further advice.

If an elected representative requests personal data from the Housing Executive on behalf of someone other than the data subject that personal data can only be disclosed if:

a. In the circumstances, the data subject cannot give consent to the processing;
b. In the circumstances, the elected representative cannot reasonably be expected to obtain the data subjects consent to the processing;
c. Obtaining the data subjects consent would prejudice the action taken by the elected representative;
d. The processing is necessary in the interests of another individual and the data subject unreasonably withholds consent.

For any disclosure of personal data to an elected representative, the decision and criteria used should be recorded.

11.6 Timeframe

Requests should be responded to without delay and at the latest within **one month of receipt**. This timeframe commences once staff are satisfied with the requestor's identity.

The time limit should be calculated from the **day after** the request has been received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

***Example**: An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.*

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, the date for response is the end of the next working day. This means that the exact number of days available to comply with a request varies, depending on the month in which the request was made.

It may be possible to extend the timeframe for response by a further **two months** where requests are complex or a number of requests have been received from the individual. If this is the case, the DSR co-ordinator should discuss the matter with the DPO. This should be done as soon as possible as the individual must be informed of the extension within one month of the receipt of the request with an explanation why it is necessary. The extension letter must be uploaded onto the DSR database.

11.7 Fees

The **first copy** of the information must be provided **free of charge**. However, a reasonable fee can be charged where a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee may also be charged where requests for further copies of the same information are received.

This does not mean that a fee can be charged for all subsequent access requests.

The fee **must be based on the administrative cost of providing the information.**

For requests where a reasonable fee may apply, please contact the DPO on dataprotection@nihe.gov.uk to discuss the request.

11.8 Processing

DSRs will be centrally maintained on a DSR database, with oversight by the DPO.

The DSR co-ordinators have the responsibility of:

a. Acknowledging the request;
b. Requesting proof of identify (if applicable);
c. Clarifying the request (if applicable).

When the DSR co-ordinator is satisfied the request is valid they must update the DSR database with the relevant information and must respond within one month of receipt of the valid request.

To process a DSR:

a. Review that the request is a DSR and not a Freedom of Information request or routine business query (divert where appropriate);

Requests received by staff members

b. For hard copy requests, date stamp the request when received, scan the request and forward to dataprotection@nihe.gov.uk ;
c. For requests received by email or via the webpage, forward the request to dataprotection@nihe.gov.uk .

Requests received by DSR co-ordinators

d. For requests received by post, date stamp and scan the request and upload to the DSR database.
e. For requests received by email, upload to the DSR database

Requests received through the data protection inbox

f. Requests will be uploaded to the DSR database and the DSR co-ordinator will be contacted and advised that a request has been received and has been uploaded to the system.

DSR co-ordinators must then:

g. Verify the identity of the person making the request, using 'reasonable means' i.e. provide proof such as an ID, or permission to act on the subjects behalf;
h. Determine if we hold the information; if so draft the response from the necessary business units;
i. Request copies of the information from the relevant business units;
j. Ensure appropriate redactions are made prior to release of information;
k. Follow up outstanding requests one week prior to their deadline;
l. Responses should be prepared using the standard letter templates found on the DSR database;
m. Seek appropriate sign off for the responses. See section 11.9;
n. Record the response date, attach the final response and associated correspondence (this must include the redacted and un-redacted copies of the information) to the database file.

Hard copy records created in the response to DSRs should be retained and disposed of in line with the Disposal of Records Schedule following the lifecycle of the record.

If a business area does not hold any personal data relating to the data subject, the DSR co-ordinator should enter this in the notes section of the DSR database and issue the data subject with an appropriate response which must be uploaded to the database. This will advise the data subject that their DSR has been dealt with and there are no records held for them.

The performance of DSR responses are reported to CXBC on an annual basis.

Guidance on use of the DSR database is available on the GDPR Gateway page.

11.9 Response Sign Off

Final responses must be signed off by a level 9 officer or their nominated representative. Where a department does not have a level 9 officer the head of the department or their nominated representative must sign off all final responses. Sign off is not required for requests for interview notes.

11.10 Access to Third Party data

Data relating to third parties means personal data relating to any person other than the data subject or the data controller. There is no right of access to information about other people (third parties) under GDPR and the DPA 2018.

The data of a third party individual can take the following forms:

a. Data supplied by another individual which relates to the data subject;
b. Details contained in the data of a data subject, which relates to someone other than the data subject.

The data controller is not obliged to disclose third party data unless:

a. The other individual has consented to the disclosure to the data subject;
b. It is reasonable in all the circumstances to make the disclosure without the consent of the other individual.

The disclosure of third party data may result in a complaint by the other individual or the data subject to the ICO if either is unhappy with the decision made. It is therefore important that all aspects are carefully considered before deciding to release or withhold another individual's data.

11.11 Response Format

The format of the response should mirror the format in which the DSR was made unless specified by the data subject, i.e. if the request is made electronically, the information should be provided in a commonly used electronic format.

At present the Housing Executive does not provide remote access to a secure self-service system. Refer to the IT team to determine if data portability is viable for the specific request and seek further advice from the DPO.

11.12 Requests for large amounts of personal data

Where a large quantity of information about an individual is processed, GDPR permits staff to ask the individual to specify the information the request relates to.

11.13 Manifestly unfounded or excessive

The Housing Executive does not have to comply with a request where it has already complied with an identical or similar request by the same individual, unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

In deciding what amounts to a reasonable interval, the following factors should be considered:

a. The nature of the data;
b. The purpose of the data processing;
c. How often the data is altered.

Where this is the case staff can consider:

a. Charging a reasonable fee, taking into account the administrative costs of providing the information;
b. Refusing to respond.

Where a request has been refused, the individual must be given a written explanation which must also inform them of their right to complain to the ICO and to a judicial remedy. This must be done without undue delay and at the latest within one month of receipt of the request.

11.14 Editing

The reply to a DSR should include all personal data that is held on a data subject at the time the DSR is received, **without amendment**.

The following are the exceptions to this rule:

a. Amendments or deletions can be made to the personal data after the DSR is received, but before a response is issued. For example, this could take the form of a change of address or bank details. In such cases the previous details may in fact be deleted from the records;
b. Personal data classified as exempt;
c. Other individual's personal data, including staff names may be withheld in certain circumstances.

Personal data must never be altered in order to make the response acceptable to the data subject when responding to their request (see section 11.15).

11.15 Redacting exempt or another individual's data

When redacting exempt or other third party data, the DSR co-ordinator must:

a. Separate those records which can and cannot be issued to the data subject;
b. Arrange to have all the records which can be issued to the data subject photocopied;
c. Ensure no deletions or amendments are made on original documents;
d. Redact any exempt data or other individual's data on the photocopies;

e. Arrange records in date order.

Decisions made by the DSR co-ordinator to withhold data must be fully documented in the decision letter and on the DSR file and database.

11.16 Potentially offensive or derogatory data

The DSR co-ordinator should identify potentially offensive or derogatory material included in the requested materials and advise the relevant manager of the imminent release of this material to the data subject.

The line manager should review and investigate the matter and take appropriate action. They should also consider what action may be required to ensure future data is recorded correctly and remind officers of the importance of not including unprofessional opinions or remarks regarding an individual in any communications.

The DSR co-ordinator should consider how best to release the data, for example, consider a meeting in the office or home visit to personally deliver the data, instead of posting it out.

The DSR co-ordinator should ensure sure the data subject receives an appropriate apology on behalf of the organisation, an explanation of their rights in relation to rectification, erasure and the right to complain to the ICO. The DSR co-ordinator should also advise the data subject of what steps are being taken to investigate and address the matter e.g. referral to the individual's line manager.

11.17 Requests to view or collect data at a Housing Executive office

The data subject can request that they view or collect their data from any Housing Executive office.

The DSR co-ordinator should make the necessary arrangements with the appropriate local business manager for the area in which the data subject wishes to view or collect the data.

Data subjects must always be accompanied when viewing original documents.

11.18 Review

If an individual is dissatisfied with the response to their DSR request, they can request a review within 2 months of the date of their response letter. The DPO will conduct the review and should aim to respond within one calendar month. An extension of up to 2 months may be required if the review is complex or there are extenuating circumstances. The review will address the initial decision with the potential for a different outcome.

The process for an internal review request must be noted in the response letter noting that requests must be sent to the DPO by email to dataprotection@nihe.gov.co.uk or by post to: DPO, Legal Services, Housing Centre, 2 Adelaide Street, Belfast BT2 8PB.

If an individual is dissatisfied with the handling (i.e. the administration) of their DSR request, this will be dealt with as a complaint under the complaints procedure and passed to the appropriate line manager to action.

Data subjects also have the right to contact the ICO directly; this must also be noted on the initial response. Letter templates are available on the DSR database.

11.19 Archiving

Closed requests will be archived on the database by the Data Protection Team after the internal review timescale has elapsed. This is 2 months after the date of the response letter.

12.0 Information Asset Register

The Information Asset Register (IAR) identifies how and what data we collect, process, hold and retain. The IAR enables us to track the organisation's information assets and their associated risks whilst removing duplication and improving efficiency. The register is held centrally by the DPO. IAOs should ensure that the DPO is advised of any required changes to the IAR.

Any changes in daily business processes will affect the IAR and should therefore be discussed with the relevant IAO and the DPO.

13.0 Breaches

A personal data breach means a breach of security leading to unauthorised disclosure or access, the accidental or unlawful destruction, loss or alteration to personal data transmitted, stored or otherwise processed.

Breaches should be reported to the DPO as soon as they are identified, by completing the breach form (this is available on the GDPR Gateway page), then scan and forward the form to dataprotection@nihe.gov.uk.

As much of the following information as possible should be detailed on the breach form:

a. Name and contact details;
b. A description of the nature of the personal data breach;
c. The categories of data and approximate number of individuals concerned;
d. The type and number of personal data records concerned;

e. A description of the likely consequences of the personal data breach;
f. A description of any measures taken to address the personal data breach.

The DPO must notify the ICO of the breach within 72 hours if he considers, based on the information given, that it is likely to result in a risk to the rights and freedoms of an individual. In addition, if the DPO considers, on the information given, that the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, he must also inform the affected individual without undue delay.

Breaches reported to the DPO will be recorded in a central database. The DPO will ensure IT Security is informed of any security breaches to enable appropriate reporting.

The Housing Executive is committed to consideration of all concerns raised anonymously, in accordance with our whistleblowing policy. Members of staff should contact the DPO if they believe they have exhausted the routes outlined in the whistleblowing policy. Details of the suspected breach can be put in writing anonymously by post or internal mail to the DPO at:
DPO, 4th Floor, Legal Services, Housing Centre, 2 Adelaide Street, Belfast BT2 8PB.

In accordance with good practice the DPO will not attempt to identify the whistle blower although this may affect the ability to investigate the breach within the scope of the details provided.

14.0 Contracts

GDPR and the DPA 2018 have brought in a number of changes that will affect the Housing Executive's commercial arrangements (both new and existing) with contractors, suppliers and consultants. There is now a requirement that any processing of personal data, by a processor, should be governed by a written contract with certain provisions included. This applies where the contract involves the processing of personal data, regardless of the value of the contract. This means that contracts which involve the processing of processing of personal data, with a value below £5,000 now require a written contract to be in place with detail proportionate to the value. Further advice can be sought from the Central Procurement Unit (CPU).

From the introduction of the DPA 1998, Housing Executive contracts have standardised clauses which include provision for contractor/supplier/consultant compliance with data protection and information laws. The Department of Finance (DoF) has issued a Procurement Guidance Note (PGN 01/18) "Actions Required on Contracts as a Result of the General Data Protection Regulation (GDPR)". The Housing Executive will address and advise on compliance with the new laws

through CPU in conjunction with relevant officers in the affected business areas as appropriate.

Under GDPR contractors, suppliers and consultants who process personal data in the delivery of their contracted work or service have their own responsibilities and liabilities.

15.0 Anonymisation and Pseudonymisation

15.1 Anonymisation

Anonymisation is the process of turning data into a form where the data subject is no longer identifiable.

This process must be used for data which will be kept for training purposes. All personal data must be removed from the file and/or case history to ensure that the individual cannot be identified. GDPR and the DPA 2018 do not apply to anonymised data.

15.2 Pseudonymisation

Pseudonymisation is the processing of personal data so that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information must be kept separately.

Where the right to erasure applies and personal data on electronic systems such as HMS, cannot be deleted due to technical restrictions, the personal data must be pseudonymised using the DSR database reference number in place of the name only and a generic address (such as the Housing Centre address), the date of birth and National Insurance Number. This process will prevent direct identification of a data subject however the data subject can still be re-identified through the use of additional information.

Pseudonymised data remains subject to GDPR and the DPA 2018.

16.0 Online Apps

Online apps will be subject to a layered approach to communicate the Privacy Notice.

Where consideration is being given to the use of online application tools that would include the processing of personal data, a DPIA must be completed as previously outlined in section 6.8. The DPIA should be discussed with the DPO to set out the data protection requirements and any controls that need to be put in place. This will be dealt with on a case by case basis in partnership with the IT department.

17.0 Further information and advice

Additional resources are available on the GDPR Gateway page.

For further advice contact the DPO (see section 2.5 for details).

Appendix 1: Glossary

Anonymisation	The presentation of data where the re-identification of the data subject is impossible.
Consent	Where a data subject actively agrees to have their data processed for explicit reasons. This must involve a positive 'opt-in' and not a pre-ticked box.
Data controller	The party who determines what data is collected, how it is used and the way in which it is processed.
Data processor	Acting on behalf of the controller, the data processor is responsible for processing data.
Data protection by design	The consideration of data protection within all projects and developments within an organisation from the outset.
Data Protection Impact Assessment (DPIA)	This is a process that should be carried out when introducing new technologies and if data processing is likely to put individuals' rights and freedoms at high risk. This could mean the large-scale processing of special category or criminal record data.
Data Protection Officer (DPO)	A DPO must be appointed as a public authority or a large-scale processor of special category data.
Data subject	The individual on which an organisation holds personal data.
Derogations	EU Member States can exercise a degree of flexibility over how to apply GDPR in certain areas.
Encrypted data	A means of encoding data using a key which renders it accessible only to users with that key.
Exemptions	These can be introduced by member states to safeguard democratic society, but must still respect the individual's freedoms and have significant grounds. More details can be found on ICO's exemptions document.
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights and data privacy for individuals. ICO enforces GDPR in the UK.
Individual rights	Enhanced under GDPR, the rights of the individual are listed as the right to be informed, to access, to rectification, to erasure, to restrict processing, to data portability, to objection and rights in relation to automated decision making and profiling. More details can be found on ICO's individual rights documents.

Lawful basis	Required for the processing of personal data, one of six lawful bases must be met before processing begins.
Personal data	Data that can be directly or indirectly linked to an individual, whether that is by name or an alternative identifier such as ID number or location information.
Personal data breach	Refers to 'a breach of security that leads to destruction loss, alteration, unauthorised disclosure of, or access to, personal data.'
Processing	Any operation or set of operations (either manual or automated) performed on personal data, including collecting, organising, structuring, storing and retrieving.
Profiling	Automated processing of personal data to make decisions or evaluations on the data subject.
Pseudonymisation	The processing of personal data so that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information must be kept separately.
Special category data	Also known as sensitive personal data, this data is deemed to be more sensitive and therefore requires enhanced levels of protection (see section 6.2 for additional processing conditions).
Data Subject Rights (DSR)	Can be submitted to organisations by data subjects in accordance with the individual rights (above).