



**POLICY & PROCEDURES:**

**HANDLING PERSONAL INFORMATION &  
THE DATA PROTECTION ACT 1998**

Version 1.0

March 2010

**Contents list**

1	<a href="#"><u>Policy Statement</u></a>	3
2	<a href="#"><u>Data Protection Procedures - Scope</u></a>	8
3	<a href="#"><u>The Data Protection Principles</u></a>	9
4	<a href="#"><u>Managing personal data as records</u></a>	10
5	<a href="#"><u>Obtaining personal data</u></a>	10
6	<a href="#"><u>Holding and using personal data</u></a>	11
7	<a href="#"><u>Keeping personal data accurate</u></a>	13
8	<a href="#"><u>Retaining or destroying personal data</u></a>	13
9	<a href="#"><u>Keeping personal data secure</u></a>	14
10	<a href="#"><u>Passing on personal data – Information Sharing</u></a>	15
11	<a href="#"><u>Data subject access and other rights</u></a>	16
12	<a href="#"><u>Third party access to personal data</u></a>	17
13	<a href="#"><u>Sending personal data out of the country</u></a>	17
14	<a href="#"><u>Further information and advice</u></a>	17
Annex A	<a href="#"><u>Glossary of data protection terms</u></a>	18
Annex B	<a href="#"><u>Data Protection Act schedule 2 - Conditions for Processing</u></a>	20
Annex C	<a href="#"><u>Data Protection Act schedule 3 - Sensitive Personal Data</u></a>	21
Annex D	<a href="#"><u>Confirming the Identity of Telephone Callers</u></a>	23
Annex E	<a href="#"><u>NILGOSC Data Sharing Agreements</u></a>	25
Annex F	<a href="#"><u>Data subject access request form</u></a>	26
Annex G	<a href="#"><u>Subject Access Request Management Procedures</u></a>	28

## 1. DATA PROTECTION POLICY STATEMENT

### 1.1 Background

1.1.1 The Data Protection Act 1998 (DPA) came into force on 1<sup>st</sup> March 2000. It supersedes and extends the provisions of the Data Protection Act 1984. Its scope was also extended by the Freedom of Information Act 2000.

1.1.2 The new Act implements a European Directive of 1995 and has two aims:

- to protect individuals' fundamental rights and freedoms, notably privacy rights, in respect of personal data processing
- to enable organisations to process personal information in the course of their legitimate business

### 1.2 Our Commitment to Data Protection

1.2.1 NILGOSC is committed to full compliance with the Data Protection Act 1998. This policy statement, and the procedures that follow, set out how NILGOSC implements the Data Protection Act 1998 (The Act) and applies it to the personal data acquired, held and used.

1.2.2 The Act applies to any processing of personal information that relates to an identifiable living individual. NILGOSC collects and uses information about the people with whom it deals. It also acquires information about others in the course of those dealings. These people, collectively called 'data subjects', includes NILGOSC employees, members of the scheme and their partners/dependants.

1.2.3 Processing includes virtually anything that can be done to information, including acquisition, storage and destruction as well as active use. The data can be factual information, such as names and addresses, or it can be expressions of opinion or intention and can occur in any format e.g. Word documents, databases, spreadsheets, emails, paper files etc.

### 1.3 The Principles of Data Protection

1.3.1 NILGOSC will follow certain procedures to ensure compliance with the eight Data Protection Principles as listed below. NILGOSC will ensure that:

- (i) Data is processed in a fairly and lawful manner
- (ii) Data is obtained only for the purposes specified and required for performance of NILGOSC duties
- (iii) Data collected is adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- (iv) Data is accurate and, where relevant, kept up to date
- (v) Data shall not be kept for longer than is necessary for that purpose or those purposes
- (vi) Data shall be processed in accordance with the rights of data subjects under the Act.

- (vii) That appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- (viii) Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

#### **1.4 Managing Personal Data as Records**

- 1.4.1 Personal data created, obtained and held by staff as a result of their work is part of NILGOSC's corporate record. These records should be managed according to the procedures and business rules which are outlined in our Document Management Policy & Procedures.

#### **1.5 Use of Data and the Fair Processing Notice**

- 1.5.1 NILGOSC will be transparent and as candid as possible when acquiring personal information from people. Any printed forms (or internet screens etc) used to obtain personal data should include a notice detailing the following:
  - Our name, in full as 'Northern Ireland Local Government Officers' Superannuation Committee', should appear somewhere.
  - A brief description of the purposes for which the information will be used. This can be a phrase or sentence such as '*This information will be used to determine eligibility for; and to calculate any pension or other benefits from, the LGPS (NI)*'. If you intend to make any additional use of the information apart from the main reason for collecting, see section 5.3 of the Data Protection procedures manual.
  - A brief description of any proposed disclosure of the information to third parties.
  - A statement that people have the right of access to information about them and the right to seek its correction.
- 1.5.2 The above is called a 'fair processing notice' and must be reasonably intelligible, in reasonably prominent type, and in a reasonably prominent position on the relevant form or screen.
- 1.5.3 NILGOSC will process personal data when justified by Schedule 2 of the Act. In general this requires obtaining consent of the data subject or ensuring that processing is essential for carrying out NILGOSC's functions or legal requirements.
- 1.5.4 Personal information will be used only for the purpose(s) for which it was obtained or for compatible purposes. For example, information collected for administration of a pension record will not automatically be used for other non-related purposes such as marketing. If information required for one purpose is being obtained, and there is any intention to use it for any further purpose, the person will be informed and asked to consent to this. The evidence of consent will be retained for as long as the personal information is used.
- 1.5.5 If the data being collected is 'sensitive' personal data (see below), NILGOSC will either obtain the consent of the data subject, or establish grounds for

carrying out the processing under Schedule 3 of the Act. NILGOSC will actively seek consent. It will not be assumed just because people have not clearly refused it.

## **1.6 Processing Sensitive Data**

1.6.1 Additional measures will be taken when processing sensitive personal data. In summary 'sensitive personal data' is data that relates to race, sexual preference, political views, religion, health, trade union membership, or criminal record.

1.6.2 NILGOSC will process sensitive personal data in accordance with Schedule 3 of the Act. For sensitive personal data one of the following justifications must also apply:

- Explicit consent has been obtained from the data subject.
- Processing is lawfully required for employment purposes or for ethnic monitoring (e.g. Equality Regulation).
- The information has already been made public by the person concerned.
- Processing is needed for legal proceedings, to obtain legal advice or to establish or defend legal rights.
- Processing is necessary to protect the vital interests of the data subject or another person and obtaining consent is not an option.
- Processing is necessary for research purposes, will not involve making decisions about the data subjects and is unlikely to cause them substantial damage or distress.

## **1.7 Keeping Data Accurate**

1.7.1 Any personal information that NILGOSC processes should be accurate and up-to-date. The difficulties of ensuring total accuracy are recognised and a realistic approach is adopted in the Act by requiring 'reasonable' steps to have been taken to ensure accuracy. The more disadvantaged a person would be through NILGOSC processing inaccurate information, the more careful NILGOSC needs to be about accuracy.

1.7.2 Data subjects have the right to seek correction of personal information that NILGOSC holds about them. If someone states that information about them is inaccurate, and can provide evidence to support this, the correction will be made.

1.7.3 When correcting personal information NILGOSC will consider whether it might have been passed to any third parties and, if so, decide whether they should be informed of the correction. If the information was disclosed to an external third party some years ago for a specific purpose, for example in connection with a mailing exercise, then sending a correction is unlikely to be necessary.

## **1.8 Retention and Destruction of Personal Data**

1.8.1 When data is no longer needed for the purpose for which it was obtained, it will be destroyed or deleted in accordance with NILGOSC's record retention guidelines. Refer to the Document Management Policy & Procedures for further details.

- 1.8.2 Emails containing sensitive personal data (for example information about someone's medical health) will not be kept in personal mailboxes indefinitely. A copy will be filed in the appropriate location (e.g. member's medical file) and the e-mail deleted when no longer needed.

## 1.9 Data Security

- 1.9.1 Personal information will be stored securely and access restricted to those with a need or right to see it. Media, including printed media, will be stored and handled in a secure fashion in order to reduce the risks from loss, unauthorised disclosure or misuse and will be disposed of securely and safely when no longer required.
- 1.9.2 NILGOSC will ensure that transmission of information, whether internally or externally, is done with a level of security appropriate to the nature of the information. All records or communications leaving NILGOSC that contain personal information such as names; addresses, National Insurance numbers etc. will be protected. Refer to NILGOSC's Information Security Policy for more detail.
- 1.9.3 Personal information will not be given out to a data subject over the telephone unless there are no doubts as to the caller's identity. If there is any doubt about the identity of the caller, the caller will be asked to put their enquiry in writing along with a verifiable signature.
- 1.9.4 In the event that unauthorised or accidental access, alteration, disclosure, destruction or loss of significant sets of personal information occurs, the circumstances will be recorded and the incident reported to the Data Protection Officer.

## 1.10 Data Sharing (including outside EEA)

- 1.10.1 Except in response to a Subject Access Request (SAR), NILGOSC will not transfer personal information about living individuals 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
- 1.10.2 Third parties who process data on NILGOSC's behalf are not directly responsible for that processing under the DPA – NILGOSC remains responsible. Where necessary a written agreement will be put in place to ensure that data is processed in line with DPA requirements and that NILGOSC's responsibility to members is discharged appropriately.
- 1.10.3 Other than through existing approved data sharing agreements, staff will not pass personal data to third parties without having first obtained approval for the transmission. Annex E of the Data Protection Procedures lists those parties that currently have agreements with NILGOSC.
- 1.10.4 Any department considering entering into new data sharing arrangement will formalise the arrangement in a 'Data Sharing Agreement'. The Data Protection Officer will retain the relevant documentation.

### 1.11 Data 'Subject Access Requests'

1.11.1 NILGOSC will make all personal data, unless covered by a specific exemption, available to individuals or their legal representatives, on request. Data subjects have the right, upon written request to:

- be informed whether or not information about them is being processed by us;
- be given a description of the information, the purpose of our processing and to whom it may be disclosed; and
- be provided with the information in intelligible and permanent form

1.11.2 To be valid, requests must be in writing. Anyone making an oral request should be asked to put it in writing and a copy of the form should be offered.

1.11.4 The Act allows 40 calendar days to respond to a SAR. This time limit is calculated from the date the SAR is received with sufficient information to validate the identity of the person making the request and any requested fee has been received.

1.11.5 NILGOSC must meet the 40 calendar day deadline to comply with the Act. Data subjects are entitled to complain to the Information Commissioner if this deadline is missed and the Commissioner will treat such breaches seriously under the Sixth Data Protection Principle.

1.11.6 The Data Protection Regulations permit a data controller to charge a maximum fee of £10 for processing a SAR; however, NILGOSC will not charge under normal circumstances.

1.11.7 All subject access requests must be co-ordinated through the Data Protection Officer. If a SAR is received elsewhere in NILGOSC, the person who receives it must contact the Data Protection Officer to advise them and make sure it is stamped with the date of receipt.

### 1.12 Further Information

1.12.1 The NILGOSC Data Protection Officer has overall responsibility for ensuring compliance with the provisions of the Data Protection Act 1998. This is currently the Information & Compliance Manager.

### 1.13 Policy Review

1.13.1 The Data Protection Policy was published in March 2010. It will be updated on an ongoing basis should the Act or NILGOSC procedure change. A comprehensive review will also be undertaken every two years, with the next review due in March 2012.

## 2. DATA PROTECTION PROCEDURES - SCOPE

- 2.1 There are sanctions to ensure compliance with the Data Protection Act. The Information Commissioner has powers to enter premises where an offence under the Act is suspected of having been committed and to inspect or seize material. The Commissioner also has the right to prosecute offenders and fines of up to £500,000 may be payable.
- 2.2 The procedures, for the collection and handling of personal information, apply to all personal information created or collected by NILGOSC and its staff in the course of their daily work.
- 2.3 Personal information includes:
- The names and other details of members, deferred members, pensioners, and other individuals with whom we do business;
  - The names and other details of those who correspond with us or provide details during telephone calls;
  - Information about contractors and suppliers of goods and services;
  - Information held by managers about their staff, such as performance management information;
  - Word processed documents, spreadsheets and databases which contain personal details such as names and addresses
  - Emails, where either the person sending or receiving is identifiable or the contents refer to identifiable people
- 2.4 Collectively this personal information is called 'personal data' and the people it is about are called 'data subjects'. The information is generally held in systems such as AXIS, TAS accounting and payroll, Outlook mailboxes, and a range of other local specific databases and files managed on the NILGOSC network.
- 2.5 NILGOSC employees are expected to do whatever is reasonably necessary to ensure compliance with the Data Protection Act 1998, and in particular to adhere to our Data Protection Procedures as set out in this manual, and to maintain confidentiality as required by the NILGOSC Code of Conduct.
- 2.6 The general rule to be followed is to handle and use information about other people as carefully as you would wish information about yourself to be handled and used. These procedures are an expansion of that general rule.
- 2.7 Some definitions of terms used in these procedures are at Annex A. The Data Protection Principles referred to in the procedures are set out in more detail below.

### 3. THE DATA PROTECTION PRINCIPLES

These Principles (which are set out in Schedule 1 to the Act) require that personal information be handled as follows:

**Principle 1:**

It shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

**Principle 2:**

It shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.

**Principle 3:**

It shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed

**Principle 4:**

It shall be accurate and, where relevant, kept up to date

**Principle 5:**

It shall not be kept for longer than is necessary for that purpose or those purposes

**Principle 6:**

It shall be processed in accordance with the rights of data subjects under the Act

**Principle 7:**

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

**Principle 8:**

It shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

## 4 MANAGING PERSONAL DATA AS RECORDS

- 4.1 Personal data created, obtained and held by staff as a result of their work are part of NILGOSC's corporate record and are subject to the procedures and business rules governing the management of records outlined in our Records Management Policy & Procedures.
- 4.2 As a general rule, the NILGOSC Data Protection Officer should be consulted about the destruction of sets of personal data. However, it is the responsibility of each member of staff to ensure that the contents of personal folders are reviewed at regular intervals. Any documents which should form part of the NILGOSC corporate record should be filed in the appropriate location within the office, or if electronic on the relevant Network Drive.

## 5 OBTAINING PERSONAL DATA

This section sets out good practice to be followed when acquiring personal information.

### 5.1 Be selective

- 5.1.1 Consider what personal information you need to collect to achieve your objective. For example when designing a form or writing a letter to someone that requests information, think about the reason you are collecting the information and ask 'What information do I really need to complete the task?' and ensure that you collect only that information. Do not collect irrelevant information simply because it might be useful at some point in the future.

### 5.2 Be open and honest

- 5.2.1 You should be as transparent and candid as possible when acquiring personal information from people. One method of ensuring this is to ensure that any form (or internet screen) used to obtain personal data includes the following:
- Our name, 'Northern Ireland Local Government Officer's Superannuation Committee', should appear somewhere.
  - A brief description of the purposes for which the information will be used. This can be a phrase or sentence such as '*This information will be used to determine eligibility for; and to calculate any pension or other benefits from, the LGPS (NI)*'. If you intend to make any additional use of the information apart from the main reason for collecting, see section 5.3.
  - A brief description of any proposed disclosure of the information to third parties.
  - A statement that people have the right of access to information about them and the right to seek its correction.
- 5.2.2 This is a 'fair processing notice' and must be reasonably intelligible, in reasonably prominent type, and in a reasonably prominent position on the relevant form or screen. It could be along the following lines:

*Northern Ireland Local Government Officer's Superannuation Committee (NILGOSC) is registered with the Information Commissioner under the Data Protection Act 1998 to hold personal information for the purpose of*

*administration of the pension scheme. Essentially the data is used to determine eligibility for; and to calculate any pension or other benefits from, the LGPS (NI). This information is held and processed by NILGOSC strictly in accordance with the Data Protection Act 1998. In order to carry out its purpose NILGOSC may receive information about members from others, such as employers, but can only do so in accordance with the law.*

*NILGOSC may, if it chooses, pass certain details to third parties who carry out administrative functions for the scheme, for example the Scheme's AVC providers and actuary. NILGOSC may also transfer information to organisations that carry out processing operations on its behalf, such as printers. Any third parties to whom NILGOSC passes personal data are also required to comply with the Data Protection Act.*

*NILGOSC is required to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds in order to prevent and detect fraud.*

*As individuals, members have a right under the Data Protection Act 1998 to obtain information from NILGOSC, including a description of the personal data which is held. Members wishing to access their data on Data Protection Act grounds should write to the Data Protection Officer at NILGOSC.*

### **5.3 Additional use of information**

5.3.1 Personal information will be used only for the purpose(s) for which it was obtained or for compatible purposes. For example, information collected for administration of a pension record cannot automatically be used for other non-related purposes such as marketing. If information required for one purpose is being obtained, and there is any intention to use it for any further purpose, the person must be informed and asked to consent to this. Retain the evidence of consent for as long as you keep the personal information.

5.3.2 In the case of sensitive personal data, consent must be active and you cannot infer consent from a failure to respond. You cannot assume consent just because people have not clearly refused it. Refer to section 6.2 for further details.

### **5.4 Be careful in creating personal data**

5.4.1 Do not make adverse comments about individuals unless they are based on recorded facts and can be defended as accurate if challenged. Whenever you write anything about individuals, remember that they have a right to ask to see what is written about them (see section 11).

## **6 HOLDING AND USING PERSONAL DATA**

This section sets out good practice to be followed when processing personal information. Processing includes holding and storing as well as actively using.

## 6.1 Be able to justify processing of personal data

6.1.1 Personal data must be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 of the Act is met. A complete copy of Schedule 2 has been placed at Annex B for reference; however, the main conditions met by NILGOSC will usually be:

- Consent has been received
- NILGOSC is required to process the data to fulfil a contract with the individual (such as the contract to administer their pension)
- NILGOSC has a legal obligation to process (e.g. due to Pension Regulations or HMRC etc)

6.1.2 If you do not have consent but you can link the processing to any of NILGOSC's statutory requirements, business objectives or targets in the current corporate plan, then you can reasonably assume that your processing is justified on the grounds that it is necessary for NILGOSC to carry out its functions. If you do not have consent or cannot make this link but need to process personal data, consult the Data Protection Officer before you start processing.

## 6.2 Processing sensitive data

6.2.1 You need to be particularly careful if you are processing sensitive personal data. A full definition of sensitive data is included in the Glossary at Annex A but in summary it is data that relates to race, sexual preference, political views, religion, health, trade union membership, or criminal record.

6.2.1 If the data being collected is deemed sensitive, you must either actively obtain the consent of the data subject to process it, or establish grounds for carrying out the processing under Schedule 3 of the Act. A complete copy of Schedule 3 has been placed at Annex C for reference. As well as needing to satisfy the requirements in section 6.1 above, one of the following justifications must also apply:

- Explicit consent has been obtained from the data subject.
- Processing is lawfully required for employment purposes or for ethnic monitoring (e.g. Equality Regulation).
- The information has already been made public by the person concerned.
- Processing is needed for legal proceedings, to obtain legal advice or to establish or defend legal rights.
- Processing is necessary to protect the vital interests of the data subject or another person and obtaining consent is not an option.
- Processing is necessary for research purposes, will not involve making decisions about the data subjects and is unlikely to cause them substantial damage or distress.

6.2.3 If none of these justifications can be used but you do need to process sensitive personal data, again consult the Data Protection Officer before you start processing.

## **7 KEEPING PERSONAL DATA ACCURATE**

This section explains the importance of keeping personal information accurate and up to date and what you should do about correcting inaccurate information.

### **7.1 Personal information should be accurate and up-to-date**

7.1.1 Any personal information that you are processing should be accurate and up-to-date. The difficulties of ensuring total accuracy are recognised and a realistic approach is adopted in the Act by requiring 'reasonable' steps to have been taken to ensure accuracy. A relevant factor is whether the person will be disadvantaged by your processing. The more this is likely, the more careful you should be about accuracy.

7.1.2 Department procedures should state the method adopted for checking the accuracy of the data you obtain and process e.g. two-tier review, or authorisation of data input / oversight processes e.g. supervisor checks.

### **7.2 Requests for correction of personal data**

7.2.1 People have the right to seek correction of personal information about them. If someone states that information about them is inaccurate and can provide evidence to support this, the correction should be made.

7.2.2 It will be necessary to record the correction and if you think there is any likelihood that you might need to refer to the previous version, or be asked when it was corrected, keep a record of the correction, for example by adding a note 'corrected on <the date>' and signing it, if it is a paper record.

### **7.3 Inform third parties of corrections to personal information**

7.3.1 If you are correcting personal information consider whether it might have been passed to another NILGOSC department and, if so, whether they should be informed of the correction.

7.3.2 If the information was disclosed to an external third party some years ago for a specific purpose, for example in connection with a job application, then sending a correction is unlikely to be necessary. If in doubt, consult the Data Protection Officer.

## **8 RETAINING OR DESTROYING PERSONAL DATA**

This section sets out the need to make decisions about keeping or destroying personal information and to implement those decisions.

### **8.1 Make retention/destruction decisions**

8.1.1 As a general rule, do not keep personal information for longer than is necessary for business requirements or through legal obligation to retain it.

- 8.1.2 If personal information is being kept as part of NILGOSC's long term business record, make sure it is saved in the archive drive (or referenced if held in hardcopy format offsite) and that it is destroyed in accordance with normal disposal schedules for that class of information. Refer to the Document Management Policy for details.

## **9 KEEPING PERSONAL DATA SECURE**

This section gives some basic guidelines about the safekeeping of personal information. See also the NILGOSC's Information Security Handbook for more detailed guidance.

### **9.1 Store personal information securely**

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

- 9.1.2 Make sure that personal information held by you is not disclosed either verbally or in writing, whether accidentally or not, to any unauthorised third party by taking the following measures:

- Do not leave paper copies of personal information where anyone else can access them. Keep manual personal records locked away securely.
- If you hold personal information on your computer, do not leave it unattended without locking the computer; do this also if you have a visitor who should not see the information on your screen.
- If the personal information is filed on the shared network drives, set access controls so that it can be accessed only by those with a need and a right to see it.

### **9.2 Transmit personal information securely**

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

- 9.2.2 If sensitive personal data is being transmitted externally by electronic means; e.g. to a contractor/supplier or other public body, the process documented in the Information Security Policy under 'Media Handling and Transmission' must be followed.

- 9.2.3 Refer also to guidance in section 10 regarding information sharing.

### **9.3 Telephone calls**

- 9.3.1 Telephone calls can lead to unauthorised use or disclosure of personal information. If you receive a call asking for personal information to be checked or confirmed, be aware that the call may come from someone pretending to be the data subject, or impersonating someone with a right of access, and check their identity. Personal information should not be given out to a data subject over the telephone unless you have no doubts as to their identity.

- 9.3.2 The caller's identity should be confirmed by asking the caller a number of questions relating to the personal information held by NILGOSC. This information can be located through the Member Summary screen in Axis. Guidance on confirming the identity of telephone callers is attached at Annex D. If you have any doubts about the identity of the caller, ask the caller to put their enquiry in writing along with a verifiable signature.
- 9.3.3 Please note that personal data can be disclosed by telephone where the enquiry is of a routine nature e.g. a member making enquiries about their benefits or requesting calculations, or a pensioner about payroll payments etc. Any other *comprehensive* requests for disclosure of personal data should be treated as Subject Access Requests and need to be made in writing. If in doubt, seek advice from the Data Protection Officer.

#### **9.4 Avoid loss, unplanned destruction or damage to information**

- 9.4.1 Ensure that unauthorised or accidental access, alteration, disclosure, destruction or loss of significant sets of personal information is kept to a minimum and, if it happens, that you record the circumstances and report the incident to the Data Protection Officer.

#### **9.5 Destroy information securely**

- 9.5.1 When deleting information held electronically, ensure that it is also removed from the Recycle Bin after deletion. Destroy paper-based personal information only under secure conditions by using a Confidential Waste bag.

### **10 PASSING ON PERSONAL DATA – INFORMATION SHARING**

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

#### **10.1 Approval**

- 10.1.1 Other than through existing approved data sharing agreements, do not pass personal data to anyone outside NILGOSC without having first obtained approval for the transmission.

#### **10.2 Record of Data Shared**

- 10.2.1 If personal data is being passed to someone outside NILGOSC, follow the guidance at 9.2 and below, and complete a Data File Control Form with the following information:
- Sufficient details of the information for it to be clearly identifiable subsequently
  - The name of the person who has authorised it
  - Details of who it has been sent and the date on which it was sent
  - The means used to send it, e.g. encrypted email
- 10.2.2 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 you are considering sharing information on a larger scale (e.g. bulk mailings), or smaller amounts of data but on a regular basis (e.g. monthly

overseas payments) then you should consider managing this process via a Data Sharing Agreement; and the following section gives guidance in this area.

### 10.3 Data Sharing Agreements

10.3.1 Third parties who process data on NILGOSC's behalf are not directly responsible under the DPA and as a consequence there is a legal requirement for NILGOSC to have a written agreement in place to ensure that data is processed in line with DPA requirements and that our responsibility to members is discharged appropriately.

10.3.2 It is a requirement that all data sharing should be registered in the NILGOSC Data Extract Control Log which is maintained by the IT department. If the data being shared is in electronic format, the responsibility for ensuring that it is forwarded to IT will reside with the person initiating transfer of the data.

10.3.3 The external transfer of information which is not 'personal data', but nevertheless is 'business sensitive' should also be managed applying the same principles set out in this guidance manual.

10.3.4 Any department considering entering into new data sharing arrangements, and those currently sharing data, are encouraged to formalise such information sharing in a formal 'Data Sharing Agreement'. The Data Protection Officer will hold the relevant documentation.

10.3.5 Annex E lists the third parties that currently have agreements with NILGOSC.

## 11 DATA SUBJECT ACCESS RIGHTS

This section outlines the rights of data subjects and how to respond to them.

### 11.1 Access Rights

11.1.1 As long as data does not fall into an *exempt data* category (see Glossary Annex A), data subjects have certain access rights:

- To be told whether information about them is being processed
- To be given a description of the information and the purpose for which it is being processed and details of others to whom it is or has been disclosed
- To see the information in intelligible form
- To be told how it was obtained by NILGOSC

### 11.2 Request Format

11.2.1 To be valid, requests must be in writing, either on a form such as at Annex F, or in a letter or email. Anyone making an oral request should be asked to put it in writing and a copy of the form should be offered.

### 11.3 Subject Access Requests (SAR)

11.3.1 All SAR's should be coordinated through the Data Protection Officer; however, a SAR can be received in any part of NILGOSC. The person who

receives the SAR must contact the Data Protection Officer (currently Information & Compliance Manager) to advise them that a SAR has been received. The Data Protection Officers procedures for handling data subject access requests are set out in a separate procedures guide attached at Annex G for information.

## **12 THIRD PARTY ACCESS TO PERSONAL DATA**

### **12.1 Requests from Third Parties**

12.1.1 There is no right of access to information about other people (third parties) in the Data Protection Act. However, the Freedom of Information Act provides a limited right of access to this information – limited by the need to comply with the Data Protection Principles and generally be fair to data subjects.

12.1.2 Requests by third parties must be in writing and should be forwarded to the Information & Compliance Manager for action under the Freedom of Information Act.

## **13 SENDING PERSONAL DATA OUT OF THE COUNTRY**

### **13.1 Transfer Zones**

13.1.1 Except in response to a Subject Access Request, do not transfer personal information about living individuals outside the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) unless:

- the data subject has given specific consent (e.g. they have provided details to enable pension payments to be made overseas), or
- a formal contract is in place between NILGOSC and the receiving party which provides equivalent protection of the rights of data subjects

13.1.2 For more information on the countries to which personal information can be exported, refer to the following Information Commissioners Guidance: [http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection/international/international\\_transfers.aspx](http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx)

### **13.2 NILGOSC Website**

13.2.1 Transfer means physically transporting the data overseas as well as providing people abroad with access to the information, for example, via the internet. We will not place on our website personal information about staff, other than names, email addresses and, in some circumstances, work responsibilities, without their consent.

## **14 FURTHER INFORMATION AND ADVICE**

14.1 The NILGOSC Data Protection Officer has overall responsibility for ensuring compliance with the provisions of the Data Protection Act 1998. This role is currently undertaken by the Information and Compliance Manager. For further information or advice please contact the Information & Compliance Manager on ext 109.

## GLOSSARY

### Component

In relation to a Subject Access Request, every clerical and computer system in every section of NILGOSC is a component.

### Data

Information about individuals which is:

- Processed on computer and/or in manual form.
- Recorded with the intention of processing on computer or manually.
- Recorded and kept electronically or manually.
- Or is recorded information held by a public authority and does not fall within the above definitions.

### Data controller

The person or body responsible for deciding what personal information is obtained and how it is to be used. NILGOSC is data controller for personal information held by it or processed under its instructions.

### Data Subject

Any individual who is the subject of personal data. This includes members, their partners and dependants and NILGOSC staff. All references to the data subject should be understood to mean the data subject or their legal representative.

### European Economic Area

The European Economic Area (EEA) consists of the European Union (EU) Member States together with Iceland, Liechtenstein and Norway. Under EEA Gibraltar is part of Great Britain. The Isle of Man and the Channel Islands are not part of the EEA.

### Effective date (In relation to a Subject Access Request)

The date on which a Subject Access Request (SAR) is received in the NILGOSC office with sufficient information to identify the data subject and the location of the data requested.

### 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.

### Exempt data

Certain data, which can be legally withheld when responding to a Subject Access Request (SAR), and which relates to: crime and taxation; medical information; and research, history and statistics. Full details of categories of exemptions can be found in the Act (see section 27 to 39 of the Act).

### External transfer

This is the passing of the SAR to another public body. On transfer to another public body NILGOSC is no longer responsible for responding to the SAR.

### Information Commissioner

This is the independent officer, appointed by Her Majesty the Queen, who reports directly to Parliament. The Commissioner was previously named the Data Protection Registrar under the Data Protection Act 1984.

**Personal data**

Data relating to a living individual who can be identified, either by the data alone or with other information or opinion held by the data controller or information likely to come into the possession of the data controller.

**Processing (In relation to data)**

Throughout the Data Protection Manual, “processing data” is defined as obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the data, including:

- Organisation, adaptation or alteration of the data.
- Retrieval, consultation or use of the information.
- Disclosure of the data by transmission, dissemination or otherwise making available.
- Alignment, combination, blocking, erasure or destruction of the data.

**Redaction**

The removal of data that is exempt by whatever means is required, for example, using black marker pen on both sides of the paper, or blanking out after photocopying the document. The original document must not be altered in any way.

**Sensitive Personal Data**

Personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

**Subject Access Requests (SAR)**

Formal written or e-mail request received from the data subject requesting sight of (or a copy of) their data record(s) held by NILGOSC (also referred to as a potential SAR if insufficient information has been received initially).

## SCHEDULE 2

### CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary—
  - (a) for the performance of a contract to which the data subject is a party, or
  - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary—
  - (a) for the administration of justice,
  - (b) for the exercise of any functions conferred on any person by or under any enactment,
  - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. — (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.  
 (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

### SCHEDULE 3

#### CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.  
(2) The Secretary of State may by order—
  - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
  - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary—
  - (a) in order to protect the vital interests of the data subject or another person, in a case where—
    - (i) consent cannot be given by or on behalf of the data subject, or
    - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
  - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing—
  - (a) is carried out in the course of its legitimate activities by any body or association which—
    - (i) is not established or conducted for profit, and
    - (ii) exists for political, philosophical, religious or trade-union purposes,
  - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
  - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
  - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing—
  - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  - (b) is necessary for the purpose of obtaining legal advice, or
  - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. — (1) The processing is necessary—
  - (a) for the administration of justice,
  - (b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order —

- (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
- (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

**8.** — (1) The processing is necessary for medical purposes and is undertaken by—

- (a) a health professional, or
- (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

**9.** — (1) The processing—

- (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
- (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

**10.** The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

## Confirming the Identity of Telephone Callers

In order to comply with the Data Protection Act, we have a responsibility to ensure we only give information out to those who are entitled to it and we are in breach of the Act if we do not do so.

### **1. How do you know if your caller is entitled to receive information?**

You need to establish the identity of the caller and be sure that it is the member you are speaking to before you release any information.

### **2. How do I establish their identity?**

To do this, you must ask them to provide 4 key pieces of information that identify them as the member. These are normally their:

- Full Name
- Address
- Date of Birth
- Member number or National Insurance number

### **3. What if they confirm a different address or other piece of data to the one on records?**

If they have moved house you should establish their address validity by asking them to provide their previous address(es) until you get a match with the one recorded in NILGOSC records.

If they cannot provide one of the above pieces of info, or what they provide you with does not match what is on our system, then you should ask them to provide another key piece of data, such as: their beneficiaries (if we have a record of them), the date they joined the scheme, employer name and address etc.

### **4. What do I say if the person does not want to answer my security questions?**

Most customers are used to being asked to confirm their personal details before information is released to them. However, if you should get a caller who is unhappy with being asked to provide information, you should explain to them that it is a legal requirement that we complete security checks and that it is to make sure that we only ever give out their personal information to them.

### **5. If the person still refuses to answer my questions, what should I do?**

If someone fails the security checks or refuses to provide the information, there is a possibility that these people are not entitled to receive the information they are asking for. You should *never* give out information if you are in doubt as to the caller's identity.

Advise the caller that you cannot provide them with any information over the telephone as they have not been able to pass the required security checks. You can offer to send a letter detailing the information requested to the address we currently hold for them. Posting the information to the address we hold will ensure that only the genuine member receives information. Otherwise the caller should be asked to place

their request in writing, so that we can verify the signature against our records before releasing the information.

## **6. What should I do if a relative or friend of a member calls?**

If you receive a call from anyone other than the member, then you need the member's permission to speak to them. If the member is with them on the call then you can speak to the member, ***complete the security checks as per above***, and confirm with them that they are happy for you to discuss their pension details with the other person. You should also establish who the caller is and add a comment to the file (on AXIS) to advise who you spoke to and what information was provided during the conversation (this should be the case for all telephone conversations held).

The authority to speak to that person only lasts for the duration of that call, so the member must always be present for you to speak to the third party.

For permanent authority, the member must send in a Letter of Authority, which must include their member number or NI number, their address and specifically name the person they wish to provide authority to. **THIS MUST BE NOTED IN A POP UP MEMO ON AXIS.** If you see the memo advising a Letter of Authority (LOA) is held for Mr. / Mrs. XXXXXXX then you may release information to that caller whenever they phone. They must, however, still complete the security questions on the *member's details* as per above.

## **7. What should I do if the caller advises me that the member is incapacitated and cannot deal with their pension or provide authority?**

In this instance we must receive a Power of Attorney, which is a legal document giving power to an individual to deal with someone's personal affairs on their behalf. We cannot release any information until this document is received. On receipt, it needs to be recorded in AXIS as per the procedure above.

## DATA SHARING AGREEMENTS IN PLACE AS AT JANUARY 2010

### Employers:

- Belfast Education & Library Board
- South Eastern Education & Library Board
- Southern Education & Library Board

### IT Support:

- Ethos
- Heywood Limited

### Medical Assessments:

- Dr A Glasgow
- Dr W R Jenkinson
- Dr D O Todd
- Dr D Turner

### Pension Provision & Support:

- Citibank Group (Overseas Payments)
- Equitable Life Assurance Society
- Prudential Assurance Company Limited
- Hymans Robertson (Actuaries)

### Printing & Distribution:

- Bradbury Graphics
- Mailroom
- Mail Matters Direct Limited
- Royal National Institute of Blind People
- RW Pierce & Co (Printers) Limited

**DATA PROTECTION ACT**

**Request for Access to Personal Information**

If you would like access to the personal data NILGOSC holds about you please complete this form and return it to:

The Data Protection Officer  
NILGOSC  
Templeton House  
411 Holywood Road  
Belfast  
BT4 2LP

**(Please use BLOCK CAPITALS)**

**I request access to personal data relating to:**

Name: \_\_\_\_\_

Member Reference \_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

Postcode: \_\_\_\_\_ Tel No: \_\_\_\_\_

E-mail: \_\_\_\_\_

Signature: \_\_\_\_\_

**This Section should also be completed if you are not the data subject:**

I confirm that I am acting on behalf of the data subject and have submitted proof of my authority to do so.

Name: \_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

Postcode: \_\_\_\_\_ Tel No.: \_\_\_\_\_

E-mail: \_\_\_\_\_

Your relationship with the data subject: \_\_\_\_\_

Signature: \_\_\_\_\_

**Details of Request**

In accordance with section 7-9 of the Data Protection Act 1998, I request access to the following personal information:

---



---



---



---



---



---



---

To assist us with our search, if you have made a former Subject Access Request please provide the date of your most recent request and any reference we may have quoted in our response to that request: \_\_\_\_\_

If you want to know answers to the following please tick the box:

- Why we are processing your personal data
- To whom your personal data are disclosed
- The source of your personal data

Our responsibilities are to:

- Acknowledge your request
- Inform you as to whether or not personal data is held
- Reply within 40 days of receiving complete request and consent

**Please Note:-**

- (1) If the information requested contains reference to a third party, NILGOSC will need to obtain their consent before releasing the information.
- (2) Certain categories of information are exempt from the Subject Access provision of the Data Protection Act and cannot be disclosed.

**For Office Use Only:**

- |                                |   |                          |
|--------------------------------|---|--------------------------|
| 1. Proof of Identity Confirmed | - (e.g. driving licence, passport, signature)     | <input type="checkbox"/> |
| 2. Third Party Representation  | - Authorisation letter received from data subject | <input type="checkbox"/> |
|                                | - Authorisation also confirmed by telephone       | <input type="checkbox"/> |

## **SUBJECT ACCESS REQUESTS: PROCEDURES FOR THE DATA PROTECTION OFFICER**

### **1. What is a Subject Access Request?**

The Data Protection Act 1998 (The Act) provides clearly defined responsibilities for data controllers regarding the processing of personal data. This applies to data held electronically or manually. The Act gives data subjects the right of access to data. This applies to NILGOSC in respect of:

- members and their representatives
- staff as employees or customers

It must be remembered that all requests for personal data received are Subject Access Requests (SARs) and have the full backing of the Act. This is regardless of the type of data requested. However requests which can be covered by normal business should be dealt with as at present.

On submission of a SAR, the data subject is entitled to:

- be told that personal data about them is being held/is not held
- be given a description of the personal data and the purpose(s) for which the data is being held
- be informed about the people or organisations or the sorts of people or organisations to whom the data may be disclosed
- be told the sources of the data held
- be provided with an intelligible copy of the data in a permanent form

### **2. Request for access to data**

NILGOSC policy is to make all personal data, unless covered by a specific exemption, available to individuals or their legal representatives, on request.

A valid SAR will not always take a standard form. The law states that you do not have to respond to a SAR unless you have received it in writing. However, an e-mail is admissible in this context. If a telephone request is received for data, you should ask the data subject to put the request in writing.

The letter or e-mail does not have to identify itself as a SAR, i.e. it does not have to include the words "subject access" or "Data Protection Act". A simple request for "information you have got on me" is sufficient to be considered a SAR. Alternatively, a SAR could be a request to have a copy of one particular document.

A data controller is only obliged to respond to a request where the data subject supplies sufficient information to enable NILGOSC to identify the:

- person making the request; and
- data requested

### **3. Ownership of the Subject Access Request**

When a SAR is received, it should be forwarded to the Data Protection Officer on the day of receipt or as soon as possible thereafter. All SAR's must be stamped with the date of receipt and the Data Protection Officer will log in a SAR Register.

The Data Protection Officer is responsible for:

- confirming the identity of the data subject and evidencing that this has been completed by attaching SAR checklist to authorisation/request
- confirming that the location of the information requested can be identified
- ensuring all necessary information is received before responding to the SAR
- ensuring all action is taken in a timely manner
- monitoring and controlling the progress of their own actions
- ensuring all responses are issued to the data subject within the 40 calendar day deadline
- responding to certain enquiries from the data subject following the issue of the response
- ensuring all actions have been fully documented in the SAR register in relation to the SAR

#### **4. Charges**

The Act allows for data controllers to make a charge for responding to SARs, subject to a maximum of £10; however, NILGOSC does not charge under normal circumstances.

#### **5. Time limits**

The Act allows 40 calendar days to respond to a SAR. This time limit is calculated from the effective date, i.e. the date the SAR is received with sufficient information to validate the identity of the person making the request and/or any requested fee has been received.

NILGOSC must meet the 40 calendar day deadline to comply with the Act. Data subjects are entitled to complain to the Commissioner if this deadline is missed and the Commissioner will treat such breaches seriously under the Sixth Data Protection Principle.

#### **6. Confirming identity**

The security requirements of the Act impose a clear responsibility on data controllers to ensure that data is not improperly disclosed. It is important therefore that false requests, by persons seeking subject access to which they have no right, are prevented.

Access will normally only be given to the data subject or someone authorised by the data subject (in writing) to receive the data. It is the responsibility of the Data Protection Officer to establish the identity of the person making a subject access request.

Where a request is made by e-mail, it is particularly important to confirm the validity of the request and 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. A signed statement is not necessarily required to provide the necessary confirmation in e-mail requests.

To enable the Data Protection Officer to identify the person, the data subject may need to provide:

- their surname, previous surname if applicable, and sufficient forenames
- their current address and any previous address if applicable

- a reference number, e.g. National Insurance Number, staff number, pension number or any other suitable identifier unique to them
- their date of birth

If the Data Protection Officer has informed the data subject of the need for further information, then NILGOSC is not obliged to comply with the request until that information has been supplied. However any such request for information must be reasonable and must not be used as a delaying tactic.

### **7. Insufficient identity details provided by data subject**

The Data Protection Officer is not obliged to respond to a SAR until all the necessary information to enable the identity check to be carried out is provided. When further information is required, the effective date does not apply, and the 40 calendar day clearance time has not begun.

If there are insufficient details, this is referred to as a potential SAR. The Data Protection Officer should contact the data subject, requesting the necessary information, and set a prompt of 30 calendar days, for receipt of the reply from the data subject.

If at the end of the 30 days no reply has been received from the data subject, issue him/her a letter explaining that since there had been no reply to our original request, we will be assuming that he/she does not wish to proceed with their request and we will be taking no further action.

Retain the SAR file for one calendar month from date of issue of final letter and then destroy it as confidential waste.

### **8. Sufficient identity details provided by data subject**

Make sure the correct effective date is entered in the file or register, as that will be the date from which the 40 calendar day time limit is calculated from.

If however, the SAR was originally treated as a potential SAR prior to this, the effective date will be the date all the necessary information is received in writing.

If, on initial receipt, the SAR contained all the necessary information to enable the Data Protection Officer to deal with it, but was not passed to him/her immediately, this will not alter the overall 40 calendar day time limit.

### **9. Withdrawal of request for access by the data subject**

There may be occasions where the data subject may withdraw the SAR. The details of the withdrawal should be recorded in the SAR file or register. The withdrawal of the SAR should be acknowledged in writing. Once this action has been completed, the SAR should be taken as cleared.

### **10. Requesting and monitoring requests for records**

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

- Manual records
- Information held on computer including e-mail
- taped conversations or their transcripts

- still photographs
- video recordings
- any other media

All formal requests will be tracked by the Data Protection Officer to ensure efficient completion.

### **11. Repeat requests**

NILGOSC 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: the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

### **12. Data subject representatives**

Disclosure of data to 'data subject representatives' should only be made where the consent of the data subject has been given or where the representative is legally empowered to act on behalf of the data subject.

If you are in any doubt about who the representative is, or whether consent is valid, you should not disclose the data. 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 e.g. a person given Power of Attorney (by a court or by the data subjects themselves) deals with all aspects of the data subject's financial affairs. If this is the case you may disclose any data to that representative that could normally be given to the data subject.

Data cannot be disclosed to someone just because he/she works for a Representative group such as CAB or welfare rights groups unless the data subject has consented.

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

- who they say they are, and
- 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, and
- asking for relevant information

### **13. Requests from members of staff/ex-employees**

Members of staff/ex-employees of NILGOSC have the same rights under the Act as members of the general public, and data can be held on them both in their capacity as employees and as data subjects of NILGOSC.

Requests from employees/ex-employees requesting personnel details should be forwarded to the Data Protection Officer as normal. The Data Protection Officer will then liaise with the Human Resources Manager.

### **14. No data held for a data subject**

It may be that a Business Area/Unit from which the data subject has requested data does not hold anything for the data subject.

In such a case the Data Protection Officer should enter this in the SAR file and issue the data subject with an appropriate letter. This will advise the data subject that their SAR has been dealt with and there are no records held for them.

### **15. Data exists but cannot be found**

If it is known that data exists but cannot be found, the Data Protection Officer must ensure the business area involved acts in a timely manner in attempting to trace missing documents.

If some data has been traced, continue normal action on that data.

If by the day before the 40 calendar day deadline, it is obvious that the missing data will not be found in time, then the data held by the Data Protection Officer should be issued to the data subject.

A letter should be issued to the data subject explaining what data has been found and apologising, as the full response has not been issued within the 40 calendar days, and NILGOSC has failed to meet the deadline.

When the missing action is completed and data has been traced, it should be issued to the data subject with an explanatory letter.

If, following a search for a missing document, the data cannot be traced, the SAR file should be updated and a suitable explanatory letter should be issued to the data subject.

### **16. Data should exist but has been destroyed in error**

If the Data Protection Officer is aware that data should exist for the data subject but has proof that it has been destroyed in error, the Data Protection Officer should write to the data subject, explaining the situation and apologising for the error.

The deadline will have been met if it is established within the 40 calendar day deadline that the data has been accidentally destroyed and either:

- that was all the data requested, or
- the other data requested had been issued within the 40 calendar days

### **17. Data Held but is being Edited**

The reply to a SAR should include all the data that is held on a data subject at the time the SAR is received, without amendment. There are three exceptions to this rule:

- Normal amendments or deletions can be made to the data after the SAR is received, but before a response is issued. For example, this could take the form of a change of address or bank details.
- Data classified as exempt is not disclosed to the data subject.
- Other individual's data, including staff names may be withheld in certain circumstances.

The data must never be altered just to make it acceptable to the data subject. If during the collection of data for the response, data is identified which contravenes any of the DP Principles, that data must be included in the response but made compliant immediately following it.

## 18. Exemptions

In certain circumstances, personal data does not have to be disclosed to the data subject in response to a SAR. The primary exemptions relate to:

- safeguarding national security
- prevention or detection of crime
- apprehension or prosecution of offenders
- assessment or collection of tax or duty
- personal data concerning physical or mental health
- personal data concerning school pupils
- personal data processed by government departments or local authorities for the purposes of social work
- regulatory functions exercised by public “watchdogs”
- journalistic, literary or artistic purposes
- research, historical and statistical purposes
- where the information is obliged to be made public under enactment
- where disclosure is required by law or made in connection with legal proceedings, etc
- parliamentary privilege
- where a claim to legal professional privilege could be maintained
- where data is processed only for personal or family affairs

Further detail on the exemptions can be seen in part 4 (sections 27 to 39) of the Act.

The Information Commissioner is critical of organisations that, while withholding data legitimately, do not quote the correct sections of the Act to support their decision. Care must be taken to fully document any decision to block exempt data. In cases where the reason for non-disclosure falls under more than one section of the Act, all relevant sections must be recorded.

Once exempt data has been redacted it may be that there is very little left on the document for the data subject to read. The document must still be issued to the data subject; otherwise NILGOSC will be in breach of the Act.

*If, when the exempt data is erased or blocked, it is still possible for inference to be drawn from the remaining data, insufficient data has been removed. It should not be possible for anyone to have any understanding of the data which is being withheld.*

Merely because information was given in confidence, or a document bears a protective security marking, is no guarantee that the information may not be disclosed. Privacy markings such as “in confidence” etc. have little effect under the terms of the Act. The requirement to disclose such documents, or otherwise, depends on the content, not the endorsement.

## 19. Data contained in E-Mail

E-mails, both incoming and outgoing, are covered by the Act if one or other of the following criteria is met:

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

Under the Act e-mails in personal mailboxes and deleted items boxes, e-mails saved onto the shared drives, and e-mails placed on paper files that fall within the definition of a relevant filing system, are all liable for disclosure in response to a SAR. Copies of deleted emails held on back-up systems may also be liable for disclosure.

## 20. Data relating to another/other individual

Another/other individual's data means personal data relating to any person other than the:

- data subject
- data controller

Another individual's data can take two forms:

- data supplied by another individual which relates to the data subject e.g. medical reports from doctors
- details contained in the data of a data subject, which relates to someone other than the data subject e.g. spouse or dependents

The rule regarding disclosure of another individual's data is that the data controller is not obliged to disclose it unless:

- the other individual has consented to the disclosure to the data subject, or
- it is reasonable in all the circumstances to make the disclosure without the consent of the other individual

The disclosure of another individual's data may result in a complaint by the other individual or the data subject to the Commissioner 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.

Each case should be considered separately. The key questions to ask, before deciding whether to disclose the information or not, are:

- **Has the other individual consented to the disclosure?**

Consideration should be given to seeking consent. It may not always be appropriate to seek consent, for example if it will mean disclosing data about the data subject to the other individual.

- **Has the other individual previously given the same information to the data subject making the request?**

NILGOSC would not be justified in withholding the data in these circumstances.

- **Is the other individual's data confidential, sensitive or harmful to either the other individual or the data subject?**

A duty of confidentiality arises in many relationships. When a clear duty of confidentiality to another individual arises, it may not be reasonable to disclose any data, which may identify that other individual.

- **Is it reasonable to disclose the data without the consent of the other individual?**

Consideration should be given to disclosing the data without the consent of the other individual: e.g. when an employer has provided wage details. However, if the employer has requested that the source of the data be withheld, consideration will have to be given to withholding their names under section 7(6a).

- **Is the other individual not prepared to consent to the data being divulged to the legal representative of the data subject?**

The other individual may be willing to consent to the data subject being given the data, but not the legal representative of the data subject. In such a case, the data relating to the other individual cannot be divulged to the legal representative. It may be appropriate to contact the data subject to advise them of this and if necessary, send the data direct to the data subject.

- **Has the other individual refused consent to the disclosure?**

If the other individual has refused consent to disclosure of the data, then this should be taken as a strong indication that the data should not be disclosed. However, the Commissioner has advised that if consent has not been given, the data controller is still required to release the data if it is reasonable in all the circumstances.

Reasonable is not defined, but if a clear duty of confidentiality arises disclosure of another individual's data without consent is unlikely to be reasonable. NILGOSC must consider the circumstances of each case, and make a judgement as to the confidentiality of the data.

Any decision to disclose data without the consent of the other individual must be fully documented.

- **Does the other individual's data contain details which will identify them? If so, will blocking be sufficient to prevent the disclosure of the other individual?**

If it is decided that the other individual's data is to be blocked, disclosure of the remaining data must be made. In this situation, the person blocking the data must be positive that the other individual cannot be identified from what will be disclosed to the data subject.

## 21. Blocking exempt or other individual's data

When blocking exempt or other third party data, the Data Protection Officer must:

- separate those records which can and cannot be issued to the data subject
- arrange to have all the records which can be issued to the data subject photocopied
- ensure no deletions/amendments are made on original documents
- block any exempt data or other individual's data on the photocopies using a black permanent marker on both sides of the paper if necessary
- arrange records in date order

Decisions made by the Data Protection Officer to withhold data must be fully documented in the SAR file.

## 22. Information supplied by doctors

Data supplied by doctors can be released to a data subject unless it has been decided it is medically harmful. If it does not contain medically harmful data, normal guidance relating to other individuals should be followed when deciding whether to release the data. In some instances it will be necessary to consult the doctor or other medical practitioner.

## 23. Potentially offensive data

The Data Protection Officer should, if they believe there is potentially offensive material included in the data which must be issued to the data subject, decide how the situation should be dealt with, e.g. consider an office interview or home visit, instead of posting the data out. Make sure the data subject understands that action is being taken to make the data compliant with the Act. Whatever the decision, the data must be made compliant, but only after issuing it to the data subject.

Consider the action required to ensure future data is recorded correctly, e.g. referral to the line manager of the staff member concerned. Inform relevant business manager about the imminent release of potentially offensive data.

## 24. Record of reasons for decision

Where it is decided that any information should be withheld and not disclosed to the data subject, the reasons and factors considered which lead to that decision should be recorded.

## 25. Actions taken by the Data Protection Officer before issuing response to Subject Access Request

On receipt of each component, ensure that:

- all data relates to the data subject
- the correct procedures for blocking exempt data are followed
- the correct procedures are carried out in relation to other individuals data
- examine them for potentially offensive data
- NILGOSC specific abbreviations have been explained
- Data which cannot be understood, e.g. because of poor handwriting, must be typed and a copy of the original document issued together with the typewritten transcript. If any part of the document is unreadable, this should be explained to the data subject and an apology included in the reply
- arrange copying of all relevant records for issue, which includes any jacket/file cover

## 26. Providing the data in permanent form

You must provide the data, of which the applicant is the subject, in permanent form unless this is not possible, would involve disproportionate effort or the data subject has agreed to accept the data in another format. Unless there is a good reason not to, you should supply paper copies.

You may provide audiotapes, videotapes or compact disks containing the data if the data subject agrees to this, or reasonably requests this. For example, you might provide a blind person with the data in audiotape form or in Braille. Generally

speaking you should not read the data out over the phone as this is not a permanent form. If further advice required, contact the Data Protection Officer.

If, after consulting the Data Protection Officer, it is decided that a permanent copy cannot be supplied, the data must still be provided in a non-permanent form.

## **27. Final action**

Ensure that the SAR file and register log is updated with relevant information at the appropriate time and authorise the release of the response to the data subject.

## **28. Method of response to the data subject**

The data subject may indicate at any time that they would like to:

- have their response posted to them
- view or collect their response personally at the NILGOSC office

If a preference is not expressed, send the response by post.

When the request is to view the originals, the data subject may request a copy of the data at the interview. This should be arranged and the copy issued by post. Make sure the letter and any envelopes are addressed correctly to the data subject.

## **29. Date of clearance of a Subject Access Request**

A SAR is cleared when the response is posted to the requestor, or the requestor is notified that it is available for them to view in the NILGOSC office.

## **30. Request by data subject to have data posted**

Prepare a covering letter to respond to the SAR. If the latest address on any computer system differs from that on the SAR, verification of the new address needs to be recorded.

This letter will accompany the data you intend to release or include a reason for data not released. The letter should cover the following areas as appropriate to the particular SAR:

- a description of the personal data of which they are the data subject
- a description of the purposes for processing the data
- information about the people or organisations, or the sorts of people or organisations to whom you might disclose the personal data
- information on the sources of the personal data
- if no data has been found, indicate this to the data subject, or if none of the data can be released, state that no data is required to be released
- an explanation of any inaccurate data being issued and details of the action NILGOSC intends to take to correct the problem
- your contact details

## **31. Request by data subject to view/collect data at NILGOSC office**

The data subject can request to view/collect their data from the NILGOSC office. The Data Protection Officer will make the necessary arrangements with the manager for the area in which the data subject wishes to view/collect data.

Data subjects must always be accompanied and not left unattended when viewing original documents.

### **32. Data subject fails to attend the appointment**

If the data subject fails to attend the appointment, the Data Protection Officer should attempt to contact him or her and make another appointment. If he/she cannot be contacted, issue the response by post.

If another appointment has been arranged and the data subject again fails to attend, issue the response by post.

If it is not possible to issue the response by post, e.g. the person is of no fixed abode, the data should be retained at the office of interview for one month from the date the Data Protection Officer tries to contact the data subject, and then destroyed.

### **33. Enquiries following a response to a Subject Access Request**

Any of the above may be disputed by the data subject, in the form of an enquiry or a request for a Review. It will be for the Data Protection Officer to decide, if he/she is the first to receive the correspondence from the data subject, whether it is a formal Review request. If it is a Review request, then it will be dealt with by the Deputy Secretary.

Enquiries following responses to SAR's will normally fall into one of five areas:

- (i) The data subject believes he/she have not received all the data held on him/her
- (ii) The data subject does not understand the data
- (iii) The data subject disputes the accuracy and/or the relevance of the data.
- (iv) The data subject finds some of the data offensive.
- (v) The data subject is unhappy that the response was not issued within the timescales allowed.

Each of these is dealt with separately below.

#### **(i) The data subject believes he/she has not received all the data held**

If the data subject believes he/she has not received all the data held, investigate the claim and reply appropriately.

#### **(ii) The data subject does not understand the data**

If the data subject does not understand the data, this may be because they do not understand the technical aspect of the data. Decide, in conjunction with a relevant expert, the most appropriate method of clearing the query.

If the data subject does not understand some of the abbreviations in the text, issue an explanation of the specific abbreviations in question.

If documents are badly handwritten (and therefore unintelligible) issue them together with a typed copy of the text. If a document cannot be deciphered, include an explanation of this in the SAR response.

#### **(iii) The data subject disputes the accuracy and/or the relevance of the data**

If there is a dispute over the accuracy or relevance of the data, this should be investigated and a decision made as to whether to retain, amend or erase the data based on the evidence provided by the data subject.

The reason(s) for the decision should be noted on the file and on any computer system records and the data subject should be notified of the reason(s) for the decision.

If the disputed data is not to be destroyed for whatever reason, for example it is correct, or accepted as incorrect but cannot be altered due to the limitations of the computer system, tell the data subject, and give a written explanation.

Once the disputed data is destroyed through the normal document retention procedures, make sure all references to it are removed from manual and computer records.

**(iv) The data subject finds some of the data offensive**

If the data subject feels some of the data is offensive, always treat this situation as a complaint and refer the matter to the Data Protection Officer.

**(v) The data subject is unhappy that the response was not issued within the timescales allowed**

The data subject may be unhappy that the response has not been issued within the 40 calendar day deadline. The response should have included an apology for missing the deadline.

When an enquiry is received following that response, tell the data subject why the deadline was missed. They should also be told that if they are still dissatisfied, they can complain to the Information Commissioner. The address of the Commissioner should be included in the reply.

**34. Data subject alleges damage and distress**

If a data subject alleges damage (or damage and distress) it can come to the attention of the Data Protection Officer;

- directly from the data subject
- as a result of an allegation made to the Commissioner

If the allegation is received directly from the data subject:

- refer it immediately, with brief details of the points at issue, to the Data Protection Officer, and
- advise the data subject that they will be contacted in due course

If the allegation is made directly to the Information Commissioner, the Data Protection Officer will contact the relevant business manager for details of the case. The request must be replied to immediately.

The Data Protection Officer will:

- formally acknowledge receipt of the allegation to the data subject
- if necessary establish the precise nature of the allegation
- liaise with the Information Commissioner
- alert Legal Representatives of NILGOSC to the possibility of litigation
- advise the business manager of the result of the allegation