National Shared Services Office

Data Protection Policy
Version :: 6/4/2022

Introduction ::

The National Shared Services Office (hereinafter referred to as the NSSO) was formally established by the National Shared Services Office Act 2017 (Number 26 of 2017). It was set up to provide to listed Public Service Bodies (PSBs), found in Schedule 1 of the Act, with certain shared services that are listed in Schedule 2 of the Act. S.I. No. 267 of 2018 provides for the delegation of said functions to the NSSO.

The NSSO is committed to protecting the rights and privacy of individuals and our clients Departments and strives for compliance with data protection legislation, including the EU General Data Protection Regulation, 2016/679 (GDPR) as given further effect in Part 3 of the Data Protection Act 2018 (Number 7 of 2018). While the NSSO acts as a controller for the purpose of its own staff and internal administration, the NSSO is a processor for the purpose of the services delivered to PSBs. This position has been reached after consultation with the Data Protection Commission (DPC) and has been determined by the Office of the Attorney General.

GDPR defines personal data as "any information relating to an identified or identifiable natural person (data subject)". This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number (e.g. PPSN), location data or online identifier and covers all electronic, manual and image data which may be held on computer or on manual files. Article 24(1) calls upon bodies not only to be compliant, but "to be able to demonstrate that processing is performed in accordance with this Regulation". This policy is part of a suite of documents, including a memorandum of understanding, our client data processing agreement and the employee handbook & privacy policy that help deliver that compliance.

Note: The key definitions used in this document as they pertain to GDPR and data protection are set out in Appendix One.

Scope ::

This policy applies to the NSSO, which for clarity includes HR, IT, Communications, Audit, Corporate Services etc, and constituent shared services centres (SSC) under its banner

- Human Resource Shared Services (HRSS)
- Pay Shared Services (PSS)
- Finance Shared Services (FSS)

This policy applies to all personal data collected, processed and stored by the NSSO in respect of all individuals, (i.e. staff, customers and service providers) by whatever means including paper and electronic records. This policy takes account of best practice in the area of data protection using resources available on the website of the Data Protection Commission and the European Commission. The NSSO currently does not have any processing being carried out in the United Kingdom or in any non-EEA country.

Recent Changes ::

Significant changes in technological developments and globalisation has seen concerns being raised in terms of the fundamental rights of the protection of an individual's personal data in the EU, and the need for a less fragmented and more modern legislature framework to address these concerns. The previous data protection regime, based on the European Union's 1995 data protection directive (Directive 95/46/EC), predated mass internet usage, hand held devices, apps, online gaming, social networking and data analytics, all of which involve the collection and processing of personal data, often for purposes that are opaque and largely unknown to the individuals concerned.

In essence, the GDPR and Data Protection Act, 2018 addresses these issues by strengthening the control individuals have over their own personal data and the purposes for which these data may be used. The GDPR standardises and strengthens the right of all European citizens to data privacy. In general, the GDPR has the following main objectives:

- harmonising and simplifying the framework for the digital single market;
- putting individuals in control of their data; and
- formulating a modern data protection governance.

At the heart of the GDPR is the requirement for organisations to be fully transparent about how they are using and safeguarding personal data, and the necessity for all organisations to be able to demonstrate accountability for their data processing activities.

Chapter 7 and in particular Section 144 of the Data Protection Act 2018 also creates an offence where "Personal data processed by a processor shall not be disclosed by the processor or by an employee or agent of the processor, without the prior authority of the controller on behalf of whom the data are processed. A person who knowingly or recklessly contravenes subsection (1) shall be guilty of an offence and shall be liable for" a significant fine or imprisonment. The offences listed in Section 144, 145 and 146 have bene brought to our staffs attention.

Data Sharing ::

The 2019 DPC guidance document "Data Sharing in the Public Sector" addressed the transfer of data between public sector bodies in terms of controller to controller relationships. While "data sharing" is not a term used in the GDPR, in its usage in this context by the DPC it was not intended to encompass the transfer of data from a controller to a processor for the purposes of enabling the processor to carry out its tasks on behalf of the controller. Article 28, which sets out the requirements for the controller-processor relationship identifies only the need for a data processing agreement, and there is no requirement for a "data sharing" agreement in this context.

The Data Sharing and Governance Act 2019 is legislation outside the data protection legislative frameworks. Section 12 of the Act provides for exclusions, notably S12(2) and (3).

> (2) Subject to Part 5, this Act shall not apply to the disclosure by a public body to another public body of the personal data of a data subject for **the internal administrative purposes** of the first or second mentioned public body.
>
> (3) The reference in subsection (2) to internal administrative purposes includes a reference to purposes relating to the employment of the data subject concerned.

For clarity, the NSSO's core function is as a processor and as such that processing relationship only needs to be covered under EU law by a processing agreement. The definition of 'data sharing' given in Section 9 of the 2019 Act arguably brings its processing into scope, however it is then exempted by Section 12.

Data Protection Principles ::

Article 5(1) of the GDPR requires that personal data is:

a) Processed in a way that is lawful, fair and transparent;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (purpose limitation)

c) Adequate, relevant and is limited to what is necessary; (data minimisation)
d) Accurate and kept up to date;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (storage limitation)
f) Processed in a manner that ensures appropriate security of the data.

Most significantly Article 5(2) of the GDPR also obliges controllers to "be responsible for, and be able to *demonstrate*, compliance with the principles". While this accountability principle applies to controllers, the NSSOs policies and procedures are designed to ensure compliance with these principles

The GDPR attaches great weight to data processing. The meaning of "*processing*" under the GDPR extends beyond the ordinary meaning that most of us associate with the word and includes the collection, recording, storage, consultation, use, adaptation, disclosure by transmission, dissemination or otherwise making available and erasure of personal data.

It essentially means anything that is done to, or with, personal data.

Under the GDPR "Processing" is defined under article 4(2) of the GDPR to mean:
"*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* ".

What are the lawful bases for processing Personal Data?

The GDPR sets out a list of 6 processing conditions under which an organisation may process personal data. One of these conditions must be satisfied for each processing activity, which an organisation undertakes. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and your relationship with the individual i.e. the "Data Subject".

Where *Special Category Personal Data* or "sensitive" personal data are processed, a separate list of processing conditions must be applied. These are set out in more detail in *Section 7* of these *Guidelines*.

The legal basis for the processing is explored further in the Department of Public Expenditure and Reform document '***DATA PROTECTION AND HR IN THE CIVIL SERVICE - Guidelines for HR managers in the civil service'***. That document states ::

"It should be noted that there is no contractual relationship involved in the service of a civil servant. Rather than serving under a contract with an employer, civil servants instead hold office by appointment under the terms of the Civil Service Regulations Acts, with a tenure at will.

This distinction is important when considering Article 6(1)(b), the contract basis. It is not recommended that this basis be used for processing under a contract of employment. See below for further details.

In the case of civil servants, the legal bases for processing and retaining HR records is found in Articles 6(1)(c) and 6(1)(f) for personal data, and Article 9(2)(b) of the GDPR and section 46 of the Data Protection Act, 2018 for special category data, to be read in conjunction with, inter alia, the Civil Service Regulation Acts, the Public Service Management Act and the Public Service Management (Recruitment and Appointments) Act, together with regulations and circulars made thereunder. It is important that Departments and Offices view the processing and retention of civil service HR data along with its obligations the National Archives Act, especially, as noted, in relation to destruction of records. "

Applying the language of data protection law to the NSSO ::

As explained the NSSO is, like every employer, a controller for the purposes of personal data is holds on its own staff and various corporate responsibilities. However, the NSSO primarily operates as a processor providing shared services to PSBs. Much of the phraseology used when discussing the responsibilities of a controller have a significantly different applications when applied to a processor. This section clarifies how the GDPR is applied in the NSSO in its functions as processor. Employees are minded to review the 'Employee Privacy Policy'

Rights of the Data Subject :: Article 12 - 23

As a processor the NSSO only hold data on behalf of client PSBs. Individuals still have a right to access the data that is held by the NSSO, but if they wish to avail of this right, they need to contact the relevant Local HR (controller PSB) in the first instance.

The NSSO will act, upon receipt of the request from the controller, in accordance with the GDPR to ensure that the requested data is returned to the data controller in sufficient time for the controller to determine which of the supplied data is appropriate to release,

Should a data subject wish to withdraw consent for the NSSO to process their information, this request must be communicated to your Local HR Office. The NSSO, as data processor, will then act in accordance with the instruction of your Local HR Office, as data controller. It important to remember that this right is only available to data subjects in certain circumstances and its application is subject to the various exceptions as outlined under GDPR.

A list of policies that deal with some of the rights in Article 12 -23 can be found in the Appendices.

Controller Responsibilities :: Article 24 – 27

As a processor the obligations of Article 24 – 27 do not fall on the NSSO. However the NSSO is cognizant of the requirements and takes particular note of Article 25, the need for data protection by design and by default. Particular attention has been given to the requirement that 'by default, only personal data which are necessary for each specific purpose of the processing are processed'.

Data Sharing Agreements ::

The principles of the applicability of data sharing to the NSSO is covered on page 2.

As a processor, the NSSO acts on behalf of client PSBs. A data-sharing agreement is a controller-to-controller document where one controller shares data with a second controller for that second controllers purposes. A data-sharing agreement therefore cannot include a processor, who by definition does not have the authority to determine the purposes and means of processing, and who under Article 28(3)(a) 'processes the personal data only on documented instruction from the controller'.

The Data Sharing and Governance Act 2019 (Number 5 of 2019) has a minimal impact on the processing carried out by the NSSO as exempted by Section 12.

Data Controller Processing Agreements :: Article 28 - 29

Article 28(3) requires that 'processing by a processor shall be governed by a contract… that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing…' etc.

The NSSO governance suite includes a Memorandum of Understanding (MOU), Employee Service Management Agreement (ESMA) and a Data Controller Processing Agreement (DCPA/DPA). Each PSB the NSSO provides a service to has received this suite of documents. The DCPA used by the NSSO was originally crafted by a team of IAPP (International Association of Privacy Professionals) members on behalf of the IAPP Privacy Bar Section. It reflects input from the IAPP global membership. It was altered for application in Ireland by members of the Civil Service Data Protection Officers Network.

The document meets the requirements of Article 28. The DCPA annex's include ::

1. Contacts details for both DPOs;
2. List of Processes to be carried out with instruction to process;
3. Security Measures
4. Transfers to sub-processors outside of Ireland / EEA (none)
5. Basis for Breach Reporting Process.
6. Third Party Service Providers

Records of Processing Activities (ROPA) :: Article 30
The NSSO has extensive process maps for each process it carries out. Those process maps have been converted into 'Article 30 records' and tailored to meet the needs of this obligation. They have been added to a list (a 'record') which is published on our website. This list should be read in tandem with details given in this section and elsewhere in this document. Together they form the NSSO's record of processing activities. Some of the required information is provided in this document for convenience to avoid duplication.

The NSSO appreciates there are different obligations on a controller [Article 30(1)] and a processor [Article 30(2)] in the preparation of the records of processing activities (ROPAs).

A30(1)(a) the name and contact details of the controller and the data protection officer ::
The contact details for NSSO and the NSSO DPO can be found below (Article 37-39).

A30(1)(b) the purposes of the processing ::
Individual purposes can be found on the published ROPA. The principle functions of the NSSO were outlined in Section 7 of the NSSO Act 2017 and references powers transferred to it under Section 8, notably the power to enter into contracts for the procurement of goods and services required for the provision of shared services. While each process is unique and has its own purpose and legal basis, the processing carried out by the NSSO where it is a controller, be it staff or office administration, are limited to functions specified in the NSSO Act and enabling legislation.

A30(1)(c) a description of the categories of data subjects and of the categories of personal data ::
This can be found on the published ROPA. As a controller the data subjects would be the NSSO employees and former staff where obligations arise, and individuals we have contracts for services with, or are engaging with for routine office administration. The categories of data are limited to what is necessary to fulfil obligations as a public service employer and contractual issues.

A30(1)(d) categories of recipients to whom personal data has been / will be disclosed ::
As a public sector body the NSSO (as a controller) has to work within certain standards and obligations common to other civil service employers. Some of these are legislative requirements, others being tied to control, audit and accountability demands. Examples where personal data might be disclosed include ::

- Freedom of Information & Data Sharing Act obligations,
- Workforce planning and pension liability assessments,
- Transfer of staff from one PSB to another.
- reporting to the Oireachtas,
- the Comptroller and Auditor General,

- other auditors as appropriately approved,
- National Archives,
- the Civil Service Employee Assistance Service, OneLearning, the Public Appointments Service etc
- authorised processors working on behalf of the NSSO for administrative or technical purposes.

This would be in addition to meeting standard employment obligations on deductions from salaries to statutory bodies (eg Office of the Revenue Commissioners, Social Protection) or authorised third parties (Trade Unions, Credit Unions, AVCs) and agents, such as auditors, acting on their behalf.

A30(1)(e) International transfers of data ::
The NSSO does not transfer personal data to third countries.

A30(1)(f) Time limits for erasure of the different categories of data ::
The NSSO, although not currently a listed body under the National Archives Act 1986, has engaged with the National Archives and is committed to meeting those standards with a view to being added as a listed body in the future. The NSSO has signed off on Document Retention guidelines, which were heavily informed by the National Archives and the guidelines produced by DPER Civil Service HR.

A30(1)(g) Technical and Security measures
While some of these would be inappropriate to disclosure, a considerable number of organisational measures have been produced for this policy.

As mentioned there are different ROPA obligations in place on a processor than on a controller. The NSSO is a processor for all the processing it carries out on behalf of other public service bodies. Data (Controller) Processing Agreements have been signed with all clients instructing the NSSO to carry out the processing activities listed on the ROPA page, subject to the legislative provisions of Schedule 2 of the 2017 Act and S.I. 267 of 2018.

A30(2)(a) the name and contact details of the processor and the data protection officer ::
The contact details for NSSO (processor) and the NSSO DPO can be found below (Article 37-39). The controller should be understood to

- the current employer;
- or in the case of former staff, the last public body that employed them;
- or in the case of retired staff re pensions, the body paying the pension.

A30(2)(b) the categories of processing carried out on behalf of each controller ::
This is as listed on the ROPA page. The high level categories are the information provided to your employer for them to comply with your employment rights, including :: contact details, age, service details, attendance (various leave types), pay details (bank, deductions, next of kin), your reporting profile (who reports to you/ who you report to) etc.

A30(2)(c) International transfers of data ::
The NSSO does not transfer personal data to third countries.

A30(2)(d) Technical and Security measures
While some of these would be inappropriate to disclosure, a considerable number of organisational measures have been produced for this policy.

In review :: The NSSO compiles a list of all processing carried out on behalf of the controllers. It is included as an Annex to the DCPA. The signature on the DCPA authorises the NSSO to carry out the processes listed in Annex 2, supporting the legislative instructions given in the delegated functions.

Breach Notifications :: Article 33 - 34
The Article 29 Data Protection Working Party adopted on 3 October 2017, as revised and adopted on 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01). The Guidelines, particularly under Section II.A.4 list obligations under Article 33 – Notification to the Supervisory Authority. This guidance (page 14) states that processors can make a notification on behalf of a controller if the controller has given the processor the proper authorisation and this forms part of the contractual arrangements between controller and processor. Such notifications must be made in accordance with Article 33 and 35 of the GDPR.

The controller PSBs have authorised the NSSO, as a processor, to notify the Data Protection Commission in line with the process agreed with in the DCPA, on the condition that the notification process is carried out in accordance with Articles 33 and 35 of the GDPR.

The NSSO in this process is also instructed to notify the controller of all breaches, irrespective of the ascertained risk to the rights and freedoms of natural persons, once the processor has concluded its investigation and fulfilled the requirements of Articles 33 and 35 of the GDPR. The NSSO does this through weekly notification of breach incident activity via secure upload to the PSB HR units. The breach reporting process can be found in the appendices.

Data Protection Impact Assessments :: Article 35 - 36
Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, a controller shall, prior to the processing, carry out a Data Protection Impact Assessments (DPIA). As a processor carrying out processing on behalf of controllers, there is no obligation for the NSSO to carry out a DPIA.

The NSSO does have an obligation under Article 28, and particularly 28(3)(f) to assist 'the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.'

Data Protection Officer :: Article 37 – 39
The NSSO DPO can be contacted by email DPO@nsso.gov.ie or ::

Adam Egan
Data Protection Officer, Assistant Principal, National Shared Services Office, Building 5, Belfield Office Park Beech Hill Road, Clonskeagh, Dublin 4, D04 A9P2
Oifigeach Cosanta Sonraí, Príomhoide Cúnta, Oifig Náisiúnta um Seirbhísí Comhroinnte, Aonad 5, Páirc Oifigí Belfield Bóthar Cnoc na Feá, Cluain Sceach, Baile Átha Cliath 4, D04 A9P2

The Data Protection Commission has published guidance on appropriate qualifications for a Data Protection Officer. Relevant skills and expertise listed includes:

1. expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
2. understanding of the processing operations carried out;
3. understanding of information technologies and data security;
4. knowledge of the business sector and the organisation; and
5. ability to promote a data protection culture within the organisation.

NSSO Data Protection Officer was appointed on April 30th 2018 and his details have been communicated to the DPC. His experience and qualifications include ::

1. Certified practitioner in Data Protection (CP.dp), Advanced Diploma in Data Protection Law from the Kings Inns, Professional Diploma in Data Protection Law and Governance (NUI) and has completed data protection courses with the IPA & IADT.
2. Has over eighteen years experience across a number of civil service departments including working in the areas of recruitment, pensions, data analysis and IT.
3. Hdip in Computer Science and Professional Diplomas in both Human Rights and Statistical Use.
4. Masters in both Public Management & Media Studies with experience of working in several civil service departments and on a variety of pan-service networks.
5. The NSSO DPO co-chairs the Civil Service Data Protection Officers Network and sits on the Data Sharing Committee of the Governments Data Governance Board.

The NSSO DPO is supported in the carrying out of their duties and does not receive any instruction regarding the exercise of their tasks. The name of the DPO has been repeatedly communicated to all staff and regular updates issue to remind staff of their duties. The DPO meets with the Management Board at least annually, and has access to bring issues to them at any time.

Data Protection Training ::

All staff have been offered training in data protection law and the undergoing of such training is mandatory for all staff who work with personal data.

Practical means will be used to ensure the impact and effectiveness of the policy. Examples include:

- Classroom style training has been made available to all staff working in the NSSO in data protection 'Principles and Procedures'
- Annual e-learning modules are mandatory for all staff who work with personal data.
- Additional
- The Information Governance/Data Protection team monitors compliance with the policy.
- Requests for access to personal data are dealt with effectively
- Personal data records are accurate and as reported from the Customer Department/PSB
- Personal data records are held securely
- Personal data records are retained only for as long as necessary.

Data Principles :: (See Data Controller Processing Agreement)

All data, including PPSN, transferred by the PSB to the NSSO and all records including those held on I.T. systems, relating to the financial, HR or payroll transactions of the PSB are the property of the PSB and are retained by the NSSO as the Data Processor and agent of the PSB. The protection of this data shall be outlined in a data controller processing agreement (DCPA) in line with the requirements of Article 28 of the GDPR. The following principles are a restatement and paraphrasing of provisions found in the DCPA, which should be treated as the primary text when being referenced.

The NSSO will process data on behalf of the PSB on the basis of the authorisation and instructions received from the PSB or the employee or as otherwise required by law and including the use of the PPSN. Any data provided by the PSB or the employee will be held by the NSSO only for the express purpose of processing the data and will not be retained or used for any purpose outside this agreement (except where otherwise provided by law).

The NSSO will process personal data in accordance with the data protection obligations of data processors as set out in data protection law.

Where the NSSO as data processor intends to outsource any aspect of the services provided under this agreement, transfers of personal data to third parties may take place only with the express written agreement of the PSB and on the basis of a written contract with the third party.

Requests for information under the Freedom of Information Act, or Subject Access Requests under the data protection law received by the NSSO will be processed in line with the process outlined at Appendix Five and in line to the data controller processor agreement. Any information in the possession of the NSSO necessary to provide a response to the request will be provided by the NSSO to the PSB. Conversely requests received by the PSB where relevant, will be re-directed formally to the NSSO.

The Customer Department/PSB shall ::

- Appoint and acknowledge the NSSO as Data Processor for the purposes of the DCPA.
- Accept primary responsibility for compliance with Public Financial Procedures, compliance with the Financial Policy Statements of the PSB and the accuracy and completeness of the financial data submitted, to the NSSO, for processing.
- Accept it is the sole decision maker for the disclosure of data and documents under both data protection and FOI law and as per the contract, expressly prohibits any disclosure of material to any third party except as by agreement.

System Ownership and Business Continuity/Disaster Recovery ::

- The NSSO oversees and has ultimate responsibility for the Business Continuity and Disaster Recovery Plans for the NSSO. These have been drawn up in consultation with the OGCIO.
- The implementation of both plans are dependant of OGCIO systems
- The NSSO has a defined system owner (OGCIO) with overall business responsibility for the operation of the system and management of all the relevant data. The NSSO has a comprehensive Disaster Recovery (DR) plan in place to ensure that it could survive a major disaster incident by recovering critical IT systems within 24 hours of a decision to invoke a disaster recovery.
- Target restore time: 24 hours or less and maximum data loss risk: 1 hour or less.

NSSO IT Platforms ::

The systems used in the NSSO fall into two categories (1) Enterprise systems such as Peoplesoft and Core, and (2) common Office Systems such as MS Office (Word, Excel, Outlook, Lync etc). Enterprise Printing, PC's, Laptops, Mobile Phones etc.

The table below illustrates the entities supporting our Enterprise systems.

System	Core Payroll	Peoplesoft HRMS
Application tier administration	Core	Bearingpoint
Infrastructure tier administration	Dept of Agriculture	OGCIO
Hosting location	ISO27001 certified Government Data Centres that are geographically diverse	

In the case of our common office environment, the Applications and Infrastructure tiers are supported and administered by OGCIO. Their various systems are housed in Government Data Centres that meet the ISO 27001 standard.

Appendix One :: Definitions & Acronyms ::

Most definitions should be assumed to have the same meaning as they have in the General Data Protection Regulation.

GDPR or "General Data Protection Regulation" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC2;

"data protection law" means
(a) the Data Protection Acts 1988 to 2003, and the Data Protection Act 2018,
(b) the General Data Protection Regulation,
(c) all law of the State giving further effect to the General Data Protection Regulation, and
(d) all law of the State giving effect or further effect to Directive 2016/680;

Data Controller or "controller" has the same meaning as it has in the General Data Protection Regulation;

Data Processor or "processor" has the same meaning as it has in the General Data Protection Regulation;

"data-sharing agreement" means an agreement between two or more public bodies (controllers) which provides for the disclosure of information by one or more of the parties to the agreement to one or more of the other parties to the agreement;

"data subject" has the same meaning as it has in the General Data Protection Regulation;

DPO or "data protection officer" in respect of a public body, means the person designated in accordance with Article 37 of the General Data Protection Regulation;

"personal data" has the same meaning as it has in the General Data Protection Regulation;

"special categories of personal data" means information referred to in Article 9(1) of the General Data Protection Regulation.

Other Acronyms ::

NSSO	National Shared Services Centre
SSC	Shared Services Centre (FSS, HRSS, PSSC)
CIS	Client Identity Services
DCPA/DPA	Data (Controller) Processor Agreement
DEASP/DSP	Department of Social Protection
DPIA	Data Protection Impact Assessment
DPA	Data Protection Acts 1988-2018
DPC	Data Protection Commission
DPER	Department of Public Expenditure and Reform
FSS	Finance Shared Service
HRSS	Human Resources Shared Service
OGCIO	Office of the Government Chief Information Officer
OL	OneLearning
PP	PeoplePoint (now HRSS)

PPSN	Personal Public Services Number
PSB	Public Service Body
PSS(C)	Pay Shared Services (Centre)

Appendix Two :: List of NSSO Relevant Policies Procedures

1.	Data breach reporting process ::	Process 0000
2.	Subject Access Request Policy (clients) ::	Process 0001
3.	Subject Access Request Policy (internal) ::	Process 0002
4.	Voice Recording Policy ::	Process 0003
5.	NSSO CCTV Policy ::	Process 0004
6.	Clean Desk Policy	Process 0005
7.	Unauthorised disclosures and offences	Process 0006
8.	Staff Photographic Identification & Photo Policy	Process 0007
9.	Cookie Policy and Website Tracking	Process 0008
10.	NSSO Third Party Release Policy	Process 0009
11.	FOI requests for Client Information	Process 0010
12.	NSSO Assisted Decision / Advocacy Policy	Process 0011 Application form
13.	NSSO deceased persons Policy	Process 0012
14.	NSSO Fraud Policy	Intranet
15.	NSSO Employee privacy statement ::	Currently online (May 2018)
16.	HR Data Retention Policy ::	DPER CS HR Policy Unit
17.	NSSO Document Management Policy ::	Under development
18.	Acceptable usage policy	OGCIO Policy on Intranet
19.	Internet Content Access policy	OGCIO Policy on Intranet
20.	Consultation & Surveys Policy	Under development
21.	Social Media Policy	Under development
22.	Mobile, USB key & Laptop Policy	OGCIO
23.	Working from Home Policy (Data Security)	Under development
24.	Business Continuity Policy	Under development
25.	Removing staff access (Ops & mobility)	Under development
26.	Employee Handbook	Given at Induction
27.	Garda Vetting Retention Policy	Under development

Civil Service Policies ::

Civil Servants work not only under a series of policies set and implemented by each employer according to their tailored business needs, but also under a set of ethical and disciplinary guidelines that apply to all civil servants. Some of these policies are listed here as they concern the standards all employees are trained and expected to comply with and are pertinent to how staff interact and use personal data they come into contact with in the carrying out of their official duties.

28.	Civil Service Code of Standards	Online at DPERs HR Portal
29.	Civil Service Disciplinary Code & handbook	Online at DPERs HR Portal
30.	Ethics in Public Office	Online at DPERs HR Portal
31.	The Official Secrets Act	Circular 15/1979
32.	Dignity at Work (accessing staff data)	Online at DPERs HR Portal
33.	PMDS & Underperformance (disclosures)	Online at DPERs HR Portal

Operating Procedures ::

I. Access to email databases procedure
II. Data communications procedure
III. Firewall management procedure – OGCIO
IV. Technology Access Safeguards
V. Patches, Anti-virus & pen testing

VI. Back-ups procedure
VII. Contractors access to server rooms

Access to email databases Procedure ::
Each user of the SSC is allocated a username and password. Passwords must be kept secure and not disclosed. The owner of a particular username is held responsible for actions taken under that username. The OGCIO can monitor stored files, email messages and internet access for auditing, investigative or security reasons. Users are only permitted to access electronic information and data that they require to perform their duties. Scenarios this might arise in ::

1. A requirement to access a staff members mail, when there is a suspicion or evidence of inappropriate use, or,
2. A requirement to access a staff members mail, when they have left the NSSO and the person replacing them needs access to their mails in order to source some information

In both cases, the current protocol would be a service desk request from NSSO HR to the OGCIO requesting the relevant access. In the case of example 2 above, the approach would be to provide temporary access to allow for sourcing of the relevant information rather than permanent ongoing access.

Data Communications Procedure ::
Other than information necessary to carry out their normal duties staff must not issue any information to third parties unless they have clear authorisation to do so. Any changes to the Data Protection Policy will be communicated to the Customer Department/ PSB's. In each SSC, all staff have been and continue to be made aware of their responsibilities with regard to policies and procedures, particularly with regard to confidentiality.

Firewall Management Procedures ::
Downloading of executable files or software within the SSC is strictly prohibited unless written authorisation is received from the IT department. The IT department shall be responsible for best practice in maintenance, upkeep and upgrading of the firewall and outlining staff compliance procedures.

Technology Access Safeguards ::
PCs and notebook computers must not be left unattended for long periods while signed-on e.g. during lunch, coffee breaks etc. Users must either logoff or activate a password-controlled screensaver. The screensaver will be set to activate by default after 10 minutes of inactivity. Confidential data held on computer media (e.g. external hard drive, flash drive) must be stored securely when not in use. Physical access to the servers will be restricted to IT administrators. All data being transferred internally or externally will have appropriate levels of security (encryption, log of ownership, etc.). Irrespective of sensitivity, data classification labels should be used to convey importance of data.

Patches and Pen testing ::
All systems are patched at both the Application layer and Infrastructure layer as deemed appropriate. The Peoplesoft HRMS system ended extended support in 2011, which means no new patches are available for that application. Regular penetration tests are performed on both the HR and Payroll systems

Back-ups Procedure ::

- The NSSO oversees BCP and DR for its People, Premises, Processes and Systems. OGCIO and the Dept of Agriculture facilitate DR by organising backup procedures and assisting with testing of DR on the NSSO's Enterprise Systems
- Ultimate responsibility for operation and management of the systems and their data rests with NSSO. OGCIO manage systems and data on our behalf

- In relation to the HRMS system the following details apply
    - Recovery Point Objective is *currently under review*
    - Recovery Time Objective is *currently under review*
- In relation to the Payroll System the following details apply
    - Recovery Point Objective is 30 minutes
    - Recovery Time Objective is half day

Contractor Access to Server Rooms ::
All contractors are obliged to sign in/out at reception/security on the day. Physical access to server rooms is by card swipe/security fob and limited to:

- NSSO Facilities Staff
- OGCIO Contractors (direct or accompanied by facilities staff, depending on location)
- Outsourced on-site security

Appendix Three :: PPSN Usage

As per Social Welfare (Consolidation) Act 2005 as amended.
http://www.welfare.ie/en/Pages/Personal-Public-Service-Number-PPS-Number-Legislation.aspx

a) The PPS Number can be used either by the public bodies named in the Social Welfare Acts or by any person or body duly authorised by these public bodies to act on their behalf.
   - The NSSO was added to Register of approved bodies under Section 74 of Data Sharing and Governance Act 2019. This provides an additional layer of transparency to the work of the NSSO.
   - In the meantime the NSSO is currently authorised to processes on behalf of client PSBs for the purposes of transactions related to the fulfilment of employer obligations.

b) The PPS Number can also be used by any person who has a transaction (see definition below) with a public body (such as the NSSO), for example an employer making Income Tax/PRSI returns on behalf of an employee.
c) While the PPS Number can only be used by public bodies, equally it can only be used by such bodies for particular transactions as follows:
   - communication or transaction
   - an application
   - a claim
   - a communication
   - a payment or
   - a supply of a service

   where the transaction relates to the public function of a public body.

NSSO use of the PPSN as an identifier ::
The NSSO has engaged with Client Identity Services in the Department of Employment Affairs and Social Protection (DEASP) for guidance where it has any concerns about the appropriate use of the PPSN in a shared services environment. It does this with a particular eye to Article 25(2) of the GDPR which states ::

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

It is important to restate that aside from its responsibilities to its own staff, the NSSO processes on behalf of other PSBs and the use of the PPSN has been determined by those bodies as controllers. This applies to the processing of HR data on behalf of employees, the processing of pay and pensions on behalf of employees and pensioners and for the purpose of payment of financial entitlements where the PPSN has been provided by sole traders or grantees in the Finance Shared Service.