National Shared Services Office

Data Protection Policy
Version :: 11/11/2020

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 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 ::
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. While Part 5 deals with 'Public Service Information', particularly pensions, section 12 (2) states '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 body.' The Act shall not affect the operation of data protection law.

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). 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 our 47 clients instructing the NSSO to carry out the processing activities listed on the ROPA page.

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 participates in the Civil Service Data Protection Officers Network.

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 monthly updates issue to remind staff of their duties.

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'
- Bi-annual e-learning modules are mandatory for all staff who work with personal data.
- The Information Governance 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.

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 bene 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	Data Controller Processor Agreement
DEASP	Department of
DPIA	Data Protection Impact Assessment
DPA	Data Protection Acts
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
PSSC	Pay Shared Services Centre

Appendix Two :: List of NSSO Relevant Policies Procedures

1. Data breach reporting process ::	Appendix Four below
2. Subject Access Request Policy ::	Appendix Five below
3. Video Recording Policy ::	Appendix Six below
4. NSSO CCTV Policy ::	Appendix Seven below
5. Clean Desk Policy	Appendix Eight below
6. Unauthorised disclosures and offences	Appendix Nine below
7. Staff Photographic Identification & Photo Policy	Appendix Ten below
8. Cookie Policy and Website Tracking	Appendix Eleven below
9. NSSO Third Party Release Policy	Appendix Twelve below
10. NSSO Employee privacy statement ::	Currently online (May 2018)
11. HR Data Retention Policy ::	DPER CS HR Policy Unit
12. NSSO Document Management Policy ::	Under development
13. Acceptable usage policy	OGCIO Policy on Intranet
14. Internet Content Access policy	OGCIO Policy on Intranet
15. Consultation & Surveys Policy	Under development
16. Social Media Policy	Under development
17. Staff Image use Policy	Under development
18. Mobile, USB key & Laptop Policy	OGCIO
19. Working from Home Policy (Data Security)	Under development
20. Business Continuity Policy	Under development
21. Removing staff access (Ops & mobility)	Under development
22. Employee Handbook	Given at Induction
23. 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.

24. Civil Service Code of Standards	Online at DPERs HR Portal
25. Civil Service Disciplinary Code & handbook	Online at DPERs HR Portal
26. Ethics in Public Office	Online at DPERs HR Portal
27. The Official Secrets Act	Circular 15/1979
28. Dignity at Work (accessing staff data)	Online at DPERs HR Portal
29. 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 is due to be added to Register of approved bodies now that the Data Sharing and Governance Act has passed into law. This will provide 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 engages 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.

Appendix Four :: NSSO Data Breach Reporting Process ::

Process Id# :: 0000
Process Name :: NSSO Data Breach Reporting Process
Date Last Updated :: 12/11/2019

Description :: Where the NSSO (processor) is made aware of a breach arising from an error made by the NSSO, it will enact the following agreed breach reporting process on behalf of the controller Public Service Body (PSB). The Article 29 Data Protection Working Party Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01), 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 34 of the GDPR. This process is considered to form such proper authorisation.

Stage 1 :: Breach Awareness & Investigation

1) Once the NSSO is alerted to a breach incident a 72 hour window commences, in line with Art 33(1).
2) All breaches will be notified to the information governance team (IGT) after which the standard IGT investigation process begins. This guidance should supplement the investigation process.
3) Within 24 hours IGT need to have a clear picture of the nature of the breach, even if the circumstances of why it happened and how to prevent it reoccurring is not resolved.
4) IGT will issue a CAPA (breach incident report) form to the section where the breach occurred.
5) The section will populate the breach incident report and return to IGT for a risk evaluation.

Stage 2 :: Breach Classification (Risk vs. No Risk)

6) The IGT will use criteria from page 9 of the DPC "breach notification form" and prior advices received from the Data Protection Commission (DPC) to determine if there is -
    a. risk or no risk,
    b. If there is a risk then to set which level of risk should apply.
7) The NSSO DPO will be made aware and consulted on all breaches at this point to make a determination on the appropriate risk level and course of action.
8) If there is a risk, then IGT will populate the DPC's "Breach Notification Form" (in line with the 2019 website submission process) within 24-48 hours of the breach being notified to them and send to the NSSO DPO and appropriate line managers for review.
9) The NSSO DPO will consult with the team and others as appropriate to finalise the wording of the breach notification form.
10) While the IGT are empowered to make determinations on such matters, particularly if the NSSO DPO is unavailable, where there is a different interpretation on any matter and especially on if a breach needs to be reported, the final determination rests with the NSSO DPO.
11) Also to be noted and connected with (10) is that a DPO has legal protections under GDPR and the Data Protection Act that other staff do not have (Art 38). Staff are encouraged to consult with the DPO if they have any concerns or wish guidance on any matters related to data protection and reporting.

Stage 3 :: Breach Notification :: DPC & controller DPOs

12) Breach notifications had issued to breaches@dataprotection.ie, but due to revisions to the DPC process are now submitted via the DPC website. This makes circulation and tracking more challenging.
13) The DPC will reply shortly with a receipt and breach code, eg BN—18-7-621.
14) Document this in your records and ensure the NSSO DPO is forwarded the notification email.

15) Any correspondence with the DPC must issue from dataprotection@pssc.gov.ie, dataprotection@peoplepoint.ie, or dataprotection.finance@nsso.gov.ie it is not to issue from personal email addresses.
16) You should always cc dpo@nsso.gov.ie on all DPC emails.
17) Any breach being notified to the DPC shall also be submitted to the controller DPO at the time of submission. The NSSO DPO will be cc'd on all PSB DPO correspondence.

Stage 4 :: Breach Notification :: Controllers :: All Breaches to LHR

18) All breaches irrespective of risk must be notified to the controller PSBs.
19) IGT will issue weekly reports, via the secure Document Management System (DMS), to the data controllers Local HR units providing details of breaches which occurred in a particular week and also provide reports where no breaches have occurred. This was previously limited to breaches in the HRSS.
20) IGT have now added breaches that occur in the payroll shared service to the DMS upload so that the report will now include all breach incidents in the NSSO.
21) LHR's who receive the secure DMS uploads will notify their DPO's or finance unit officials as appropriate.

Stage 5 :: Breach Notification :: Data Subjects

22) The NSSO will notify data subjects of a breach where the risk is deemed as high or severe, in line with data protection law, DPC advice and best practice. Attention is particularly drawn to Article 34(1).
23) The NSSO will not be notifying data subjects of a breach where the risk is deemed as non-existent, low or medium, as a matter of routine. Attention is particularly drawn to Article 34(3)(b).
24) Where a DPO of a client PSB requests that data subjects are notified of a no/low/medium risk breach, the NSSO will issue agreed correspondence in line with Article 34(2).

Assessing Risk ::

The NSSO is obliged to report a breach where is presents a risk to the affected individual. Risk should be determined by the impact it could have on the data subject. In assessing the potential impact you should consider the type of breach, to who the data is exposed, if the data has been accessed and/or contained.

- No Risk : The breach will not have an impact on individuals, the data has been contained and in a Civil Service context the DPC have advised :: *'if you consider the recipient "trusted", this may eradicate the severity of the consequences of the breach but does not mean that the breach has not occurred. However, this in turn may remove the likelihood of risk to data subjects, thus no longer requiring notification to the DPC'.*

- Low : The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- Medium : The breach may have an impact on individual, but the impact is unlikely to be substantial
- High : The breach may have considerable impact on affected individuals
- Severe : The breach may have a critical, extensive or dangerous impact on affected individuals.

Risk Summary ::

- No risk breaches will be notified to the LHR only via the weekly DMS upload.
- Low & Medium risk breaches must be reported to the DPC and will be notified to the LHR and PSB DPO.
- High & Severe must be communicated to the DPC and to the data subject and will be notified to the LHR and PSB DPO

Appendix Five :: Subject Access Requests

Process Id# :: 0001
Process Name :: NSSO Subject Access Request Process (Clients)
Date Last Updated :: 21/3/2019

Description ::

Chapter III of the GDPR sets out the 'Rights of the data subject. Article 15 sets out the standards that must be met to ensure 'Rights of access by the data subject'. It states ::

'15 (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:'

'15 (3) The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.'

Receipt of a subject access request from a data subject ::

As the NSSO operates as a processor on behalf of controllers, it is important all data subjects initially direct their Subject Access Requests (SARs) to the appropriate controllers. As a controller they have ultimate responsibility for compliance with the Regulation and determine which material should be released and which should not.

As a processor the NSSO has no legal discretion or authority to release any data under a SAR to anyone but the controller. Therefore the NSSO cannot accept any SARs that should legally be directed to a PSB. Where such a request has been received the NSSO will inform the data subject of that fact and direct the data subject to make contact with the PSB.

SAR request to a PSB :: SAR process and the NSSO obligations

The NSSO is aware of the short window for compliance with a valid SAR and is committed to providing requested material to our PSB clients within a window that enables the controller to fulfil their legal obligations.

1. The data subject will submit a valid SAR to the appropriate controller PSB.
2. The PSB will evaluate the request to determine where the material lies.
3. If the PSB decides the NSSO may have material to contribute to the request it will request the NSSO to provide that data to them.
4. The NSSO aims to provide that material within 20 days to the controller.
5. The controller will assess the material provided by the NSSO.
6. The controller is the sole body entitled to determine what material shall be released, redacted or refused and shall be the sole body communicating with the data subject on said maters.

Process Id# :: 0002
Process Name :: NSSO Subject Access Request Process (Internal)
Date Last Updated :: 11/10/2019

Description ::

Chapter III of the GDPR sets out the 'Rights of the data subject. Article 15 sets out the standards that must be met to ensure 'Rights of access by the data subject'. It states ::

'15 (1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:'

'15 (3) The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.'

Receipt of a subject access request from a data subject ::

The NSSO operates as a controller on behalf of its staff and own organisational data, it is important all data subjects initially direct their Subject Access Requests (SARs) to the appropriate division. As a controller the NSSO has responsibility for compliance with the Regulation and determine which material should be released and which should not.

Please note: if you are a relative/representative requesting information on behalf of the person concerned, you must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone, you must confirm your capacity to act on their behalf and explain why you are entitled to access their information.

Format of a valid SAR request to the NSSO ::

The NSSO is aware of the short window for compliance with a valid SAR and is committed to providing requested material to data subjects within a window that complies with the Regulations.

1) The data subject will submit a valid SAR to NSSO HR at NSSOResourcing@per.gov.ie. It should be noted that a SAR can technically be made to any staff member, but that staff member should immediately refer it to NSSOResourcing@per.gov.ie.
2) The data subject will be asked to complete a Personal Data Access Form so that the request is clearly defined. Again this is not a legal requirement and cannot be insisted upon, but it removes any ambiguity to the request.
3) The NSSO will then take reasonable and proportionate measures to verify the data subjects identity, as per Recital 64. Once the identity has been confirmed the SAR is considered valid and the clock begins (see 11.)
4) The NSSO does not charge a fee for Subject Access Requests.
5) If it is considered by NSSO HR that more information is needed, you may be asked to clarify your request to enable them to respond appropriately.

6) The NSSO HR will gather any manual or electronically held information and identify any information provided by a third party or which identifies a third party.
7) When responding to a SAR that involves providing information that relates both to the individual making the request and to another individual, NSSO HR is not obliged to comply with the request if to do so

would mean disclosing information about another individual who can be identified from that information, except where:

a. The other individual has consented to the disclosure; or
b. It is reasonable in all the circumstances to comply with the request without that individual's consent
c. The release of the data will not adversely affect the rights and freedoms of others, as per Article 15(4).

8) The decision to disclose will be based on balancing the data subject's right of access against the third party's individual rights in respect of their own personal data as per Article 15(4). If the third party consents to disclosure then it would be unreasonable not to do so. However, if consent is withheld, NSSO HR will need to consider the following in deciding what may be disclosed. NSSO HR will decide whether it is 'reasonable in all the circumstances' to disclose the information and will consider the following in deciding what may be disclosed:-
    a. Is there any duty of confidentiality owed to the third party;
    b. Any steps we have taken to try and obtain third-party consent;
    c. Whether the third-party is capable of giving consent; and
    d. Any stated refusal of consent by the third-party.
9) Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent, by NSSO HR to you. GDPR does not change the current options of format available to you: i.e. electronic version or paper file.
10) Any complex terms or abbreviations contained in the information will be explained or defined when it is shared with you.

11) The GDPR allows for a period of one month, starting from when we have received all the information necessary to identify you (as per point 3), to identify the information requested, to provide you with the information or to provide an explanation about why we are unable to provide the information.
12) NSSO HR may extend the time to respond to your SAR by a further two months if the request is particularly complex or if you have placed several requests.
13) Should an extension be required, NSSO HR will contact you without delay and at least within one month of receiving the request in order to explain why an extension is required.
14) If you have made a previous subject access request, the NSSO may consider if a reasonable interval has elapsed since the previous request, in line with the provisions of Article 12(5). A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

15) GDPR does not alter your existing right to update data held about you. If NSSO HR agrees that the information is inaccurate, they will correct it and where practicable, destroy the inaccurate information. NSSO HR will also consider informing any relevant third party of the correction.
16) If NSSO HR does not agree or, if it feels unable to decide whether the information is inaccurate, a note of the alleged error will be made and kept on file

17) If you need any further information, or updates on your SAR, you can contact NSSO HR for further details.
18) You may also contact the Data Protection Officer of the NSSO, Adam Egan at dpo@nsso.gov.ie or the team at dataprotection@peoplepoint.ie.
19) Should you remain dissatisfied, you have the right to refer the matter to the Data Protection Commission at:

1. Data Protection Commission
2. Canal House, Station Road, Portarlington, Co. Laois,
3. R32 AP23
4. info@dataprotection.ie

20) This policy will be reviewed periodically so as to ensure continued compliance with relevant legislation. Policy reviews will be undertaken by the Data Protection Officer and other internal stakeholders.
21) SARs will be kept on file for a year. This is to assist in where a series of requests are received which potentially could be viewed as vexatious or repetitive in nature.

Appendix Six :: Voice Recordings

Process Id# :: **0003**
Process Name :: **NSSO Voice Recording Policy**
Date Last Updated :: **14/5/2019**

Description ::

Article 5 of the GDPR sets out the principles relating to processing of personal data. Amongst the requirements are that personal data be processed transparently, for specified and explicit purposes, limited to what is necessary and retained only as long as necessary.

The NSSO has an interactive voice response (IVR) telephone system that is capable of recording conversations. Like many other organisations, this is a standard practice that allows the recording of telephone calls for quality monitoring and training purposes. Incoming calls received via the IVR are recorded by the Shared Services Centre's (SSC) in the NSSO and this is notified to callers at the time the call is connected to the IVR. These recordings will only be used for the purposes specified in this policy.

The call recording facility is automated and only accommodates incoming calls received from outside by the SSC through the IVR only (Main number). Outbound calls to people made from the Shared Service Centre will not be recorded. If calls are transferred within the SSC, the call recording will continue until the call is ended.

Purpose ::

The NSSO in delivered its service records phone calls. This is done for the following reasons ::

a) staff training, coaching and support,
b) to monitoring the quality of call handling and customer service,
c) verification of what was said during a phone call if there is a dispute or complaint,
d) to protect staff from abusive behaviour, and
e) to verify the customer's agreement during certain service requests as appropriate.

Access & Control ::

The conversations are recorded by a third party telecoms provider and uploaded to a secure server on the OGCIO system.

HRSS Calls :: hold the naming convention :: YYYY_MMDD_HHMMSS_NSSONumber_CallerNumber.
PSSC Calls :: hold the naming convention :: 1151_YYYYMMDD_HHMMSS_450839 (a database ref number)

Access will be granted under a Subject Access Request from a data subject once it complies with the policy listed below.

Access by the NSSO for the reasons listed above in 'Purpose' will be limited and strictly controlled. Permission to access those recordings must be requested from the manager of the of the call centre in PSS or HRSS.

Access permissions to the IVR folders are managed and only named mangers in service management and the contact centre can access the recordings.

Retention Period ::

HRSS Calls :: retained for six months.
PSSC Calls :: retained for three months.

The NSSO notes that recordings of calls contain personal data and sometimes special categories of personal data. The recordings will be retained for the above stated period unless known to be needed for any of the above listed 'purpose of recording' examples. In such an event the file will be copied for continued access. All other files will be deleted.

Subject Access Request to a voice recording :: NSSO obligations & process

The NSSO will release any held voice recordings on data subjects through the standard Subject Access Request policy to the controller. To identify any calls the data subject will need to make known the date and approximate time of the phone call so it can be located as calls are not linked

1) The data subject will submit a valid SAR to the appropriate controller PSB.
2) The PSB will evaluate the request to determine where the material lies.
3) If the PSB decides the NSSO may have material to contribute to the request it will request the NSSO to provide that data to them.

4) If access to a voice recording is sought then the NSSO will need the date and approximate time of the call and, if possible, the number the data subject dialled from.
    a. This is to facilitate location of the file which is not mapped to a customers file.
5) The NSSO aims to provide that material within 14 days to the controller.

6) The controller will assess the material provided by the NSSO.
7) The controller is the sole body entitled to determine what material shall be released, redacted or refused and shall be the sole body communicating with the data subject on said maters.

Appendix Seven :: NSSO CCTV Policy

Process Id# :: **0004**
Process Name :: **NSSO CCTV Policy**
Date Last Updated :: **28/4/2019**

Description ::

Article 5 of the GDPR sets out the principles relating to processing of personal data. Amongst the requirements are that personal data be processed transparently, for specified and explicit purposes, limited to what is necessary and retained only as long as necessary. The NSSO is a controller for the purpose of its own staff. These staff are housed in a number of building across the country. These are ::

	Location	Controller/ Landlord	CCTV
1	Trinity Point (Corporate)	OPW	
2	Clonskeagh (HRSS)	NSSO HRSS	Locations listed below
3	Mount Street (FSS)	OPW / Revenue	
4	Tullamore Block 2 (PSS / FSS)	OPW	
5	Galway (PSS / FSS)	Dept of Defence	
6	Deepark, Killarney	OPW	
7	Gov Offices, New Road, Killarney	D/Culture, Heritage & G	

The NSSO is a tenant in each of the locations but only has a controller function in relation to CCTV at the Clonskeagh office. Queries relating to CCTV operations at the other sites should be referred to the landlords listed above.

Purpose of Processing ::

The NSSO carries out CCTV surveillance exclusively for the following reasons ::

I. Security of the premises
II. The system will typically be intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

Security Arrangements ::

The storage medium is stored in a secure environment with a log of access kept. Access is restricted to authorised personnel. The authorised personnel are,

- the **EO** in Facilities: (as of 1/1/2019) John McVeigh.
- The **CO** in Facilities: (as of 1/1/2019) Hugh Roberts.
- The **CO** in NSSO HR: (as of 1/1/2019) Aoife McDonnell.

Access & Control ::

CCTV footage may be provided to ::

I. NSSO / HRSS Senior Management Team,
II. An Garda Síochána.

The Data Protection Commission considers that requests for downloads of CCTV footage made by An Garda Síochána to third parties should be followed up in writing at all times. Any such requests should be on An Garda Síochána headed paper, quoting the details of the CCTV footage required and should also cite the legal basis for the request. It must be signed by a Garda at the level of Superintendent or above.

There is a distinction between a request by An Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

Retention Period :: 30 Days

Article 5(1)(e) of the GDPR states that personal data "shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data processed". A "Data Controller" needs to be able to justify this retention period.

NSSO's standard period of retention is 30 days, except where an issue has been identified, such as a break-in or theft. In such an event the footage may be retained specifically in the context of an investigation of that issue at the determination of NSSO Senior Management and / or the Data Protection Officer.

Access request to CCTV :: NSSO obligations

Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage. To exercise that right, a person must make an application in writing. This service is free of charge. The NSSO will respond to such a request within a month.

1. Applications in writing must be made to the Information Governance Team in HRSS, who will decide the validity of the application and will issue an instruction to the authorised personnel in facilities to provide the requested information.
2. Any individual making a request shall supply the NSSO with such information as it reasonably requires in order to satisfy themselves of the identity of the individual e.g. Valid Passport or Driving License.
3. When making an access request for CCTV footage, the requester should provide the NSSO with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the approximate time and the specific date(s) on which their image was recorded.
4. If the recording no longer exists on the date on which the NSSO receives the access request, it will not be possible to get access to a copy. Requesters should be aware that CCTV footage is typically deleted within 30 days of being recorded.
5. For the NSSO's part, the obligation in responding to the access request is to provide a copy of the requester's personal information, typically providing a copy of the footage in video format (DVD).
6. Where images of parties other than the requesting data subject appear on the CCTV footage, the NSSO will pixelate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requestor.
7. Alternatively, the NSSO may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.

Camera Locations :: Clonskeagh Office

1. Outside Main Door
2. Inside Main Door Lobby
3. Car Park -2
4. Car Park -1
5. Car Park -1
6. Back Door Outside
7. 1st Floor Lobby
8. Ground Floor Back Door Lobby
9. Emergency Stair Well 1st Floor
10. Comm's Room 1st Floor
11. Ground Floor Secure Room outside Emergency Stair Well Exit.

Appendix Eight :: NSSO Clean Desk Policy

Process Id# :: 0005
Process Name :: NSSO Clean Desk Policy
Date Last Updated :: 18/5/2019

Description ::

To ensure the security and confidentiality of personal data and all other work related information, the National Shared Service Office (NSSO) has adopted a Clean Desk Policy for all desks, computers, devices and printers/photocopiers.

This policy ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will minimise the risk of unauthorized access, loss of, and damage to personal data and any other information during and outside of normal business hours or when workstations are left unattended.

A Clean Desk Policy is an important security and privacy control and necessary for data protection compliance. This policy applies to all permanent, temporary and contracted staff working for or within the NSSO.

Policy ::

At all times, the following will apply:

- **All hardcopy and electronic data** must be kept secure.
    - Hardcopy items must be locked away in the relevant drawer or filing cabinet when desks are unoccupied and when the items are no longer in use.
    - Electronic files must be password protected at all times.
- **Computers** must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- **Filing cabinets** must be kept closed and locked when not in use.
- **Laptops and mobile devices** must be secured when not in use, and removed from the desk and locked away in a drawer or filing cabinet.
- **Keys** for accessing drawers or filing cabinets should not be left unattended at a desk.
- **Passwords:** All passwords must be kept secure. No passwords may be written down.
- **Printers:** Any print jobs must be retrieved immediately. When printing, ensure that you are sending items to the correct printer.
- **Disposal of data:** All unnecessary paperwork left over at the end of the work day will be properly disposed of. Such data must be disposed of securely. Hardcopy items must be disposed of using confidential waste bags or shredding machines. Under no circumstances should such items be placed in regular waste paper bins.
- **Storage devices** such as USBs must be password protected and locked away when not in use.

Compliance ::

This policy will be officially monitored for compliance by line managers, the information governance team or Data and may include random and scheduled inspections.

Non-Conformance ::

All policies require the participation of staff and contractors to be successful. Any employee or contractor found to have violated this policy may be subject to disciplinary action.

Appendix Nine :: Unauthorised Disclosure and Offences Policy

Process Id# :: 0006
Process Name :: Unauthorised Disclosure and Offences Policy
Date Last Updated :: 1/7/2019

Description ::

Article 84 of the GDPR sets out that Member States shall lay down role for penalties for infringements of the Regulations. A list of offences are listed in Chapter 7 of the Data Protection Act and are duplicated below. In review it shall be an offence to ::

1. (144) knowingly or recklessly disclose personal data received by a processor, including any employee, to another party without the prior authority of the controller.

2. (145) obtain access to personal data and disclose that data to another person without authorisation. Additional offences include selling personal data or offering to sell personal data.

3. (146) have the body corporate carry out an offence under the Act "committed with the consent or connivance of, or to be attributable to any neglect on the part of" a person of significant responsibility and they will be punished as if guilty of the original offence.

Beyond reputation damage to the organisation and any disciplinary matters arising, there are potentially serious consequences upon conviction of each offence including imprisonment or a fine.

It is important any person acting on behalf of the NSSO and handling personal data respects the gravity of the offence and complies with the data protection policies as advised.

Offences under Chapter 7 of the Data Protection Act

Unauthorised disclosure by processor

144.(1) 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.

(2) A person who knowingly or recklessly contravenes subsection (1) shall be guilty of an offence and shall be liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(3) Subsection (1) does not apply to a person who shows that the disclosing concerned was required or authorised by or under any enactment, rule of law or order of a court.

Disclosure of personal data obtained without authority

145. (1) A person who, without the prior authority of the controller or processor—

(a) obtains personal data, and

(b) discloses the data or information to another person,

shall be guilty of an offence and shall be liable—

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(2) Subsection (1) does not apply to a person who shows that the disclosing was required or authorised by or under any enactment, rule of law or order of a court.

(3) A person who sells personal data that were disclosed to the person in contravention of subsection (1) shall be guilty of an offence and shall be liable—
(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

(4) A person who offers to sell personal data obtained without the prior authority of the controller or processor shall be guilty of an offence and shall be liable—
(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
(b) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both

Offences by directors, etc., of bodies corporate

146. Where an offence under this Act is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

Appendix Ten :: Subject Access Requests

Process Id# :: 0007
Process Name :: Staff Photographic Identification & Photo Policy
Date Last Updated :: 4/7/2019

Description ::

The NSSO requires all staff employed by the NSSO on a permanent, temporary or on a contracted basis including through a third party contractor, to submit to photographic identification.

The Data Controller for the photographic images is the National Shared Services Office.

Purpose of Processing ::

This requirement is to fulfil the its responsibilities, under Health, Safety and Welfare at Work Act 2005, to all staff, and to ensure the security and integrity of information, held at offices, in line with its responsibilities under Data Protection legislation.

The photograph will be used for the purposes of staff identification and will be displayed on the integrated staff identification card/access control card/flexi card/managed print card and/or the Department Authorised Officer Card. If a staff member wishes, it will also be available for use on the internal phonebook through an "opt in" facility. The placing of the photograph on the phone book is entirely voluntary. Consent may be withdrawn at any time.

The NSSO has undergone a lot of growth and change in recent years with significant staff mobility. As a way of bringing people closer together and enabling people to put faces to names, it is intended that the phonebook/organisation chart be updated to enable staff ID photographs to be displayed along with the previously available information. The placing of your photograph on the phone book is entirely voluntary. You may withdraw your consent at any time. Senior staff should also note that data is drawn from the NSSO to populate the 'Who Does What' website.

Access & Control ::

The issuing of these cards on which the photographic ID is printed is dealt with by a small dedicated Unit in HR division. The photographic images are held on the Department Network, on a secure server, with access limited to the staff in the dedicated Unit in HR

Staff using the 'Lync' system and choose to replace the standard grey/white peg icon with an photograph of their choice. By placing a photograph here staff should be aware the photograph will sync with Outlook and present to others on the same platform. The NSSO has now asked staff to utilise this feature and so staff use it are being deemed to have knowingly consented to using it in a professional capacity and should be aware emails featuring such images may form part of disclosures in FOI and other legal obligations. Images should comply with all dignity at work principles.

Principles of Use ::

- The photographs will not be shared or used for any other purposes unless with the express consent of the individual.
- The photographs will only be held for the duration of employment. When a staff member leaves the NSSO, HR will delete their photo. The NSSO will put in place arrangements for the updating of staff photographs.

- All queries regarding the use of the photographic image should be directed to the HR Division at the following email address xxxx@nsso.gov.ie

Frequently Asked Questions ::

Why would the NSSO like me to put my photo on the internal phonebook / Lync-Outlook?
Photographs on the phone book put a human face to the name when dealing with your colleagues, which is particularly pertinent in a geographically dispersed organisation like the NSSO. This has been proven to enhance communication between staff on every level in successful organisations, and allow for stronger working relationships.

Is it compulsory to put my photo on the phonebook / Lync-Outlook?
No, this process is entirely voluntary.

I do not want my photo on the phonebook anymore, what now?
You can revoke your consent at any time and your photo will no longer appear on the phonebook. Just contact dataprotection@peoplepoint.gov.ie

Is it just for internal use or will the general public be able to see my photo?
The phonebook can only be accessed on the OGCIO shared service platform so the general public will not have access. Colleagues in other OGCIO shared email platforms (DPER, D/Finance, D/RCD) will have access to photographs you choose to use in the Lync/Outlook client.

Where is my photo coming from?
Staff photos are held on a secure server that is only accessed by a small number of members of the HR Division. Through consenting to your photo being used, the phonebook draws your photo from this server and places it on your profile. It identifies each individual through their computer log-on name. At no point in this process does this photo leave the server, and nobody else has access to your photo.

How can I change my photo?
If you wish to update your photograph with the HR Division, you may do so in the following ways:

- A high quality jpeg image may be sent as an attachment to dataprotection@peoplepoint.gov.ie
- Arrange an appointment with HR to have your picture retaken. You can do this by emailing your request to: dataprotection@peoplepoint.gov.ie

If I change my photo, how long will it take to update on the phonebook?
Once your photo is placed into the secure server by Services, Health and Safety Division, it will update automatically on the phonebook.

If I leave/retire/transfer from the NSSO what happens to my photo?
Your photo is deleted from the server, and automatically removed from the phonebook.

How long is my photo held for?
Your photo is only held for the duration of your employment with the NSSO. Once you leave, your photo is deleted.

Can other staff members use my photo?
No. Photographic images are personal data. Explicit written consent from the staff member is needed to use a photo for any reason other than the staff ID cards. The copying or usage of staff photographic images from the phonebook without the explicit consent of the individual in question is a breach of their data protection rights and may result in disciplinary procedures.

The Department's Disciplinary Procedures may be invoked if photos are used from the phonebook without the consent of the individual in question**.**

Is there something to stop another staff member from using my photo for other purposes anyway?
Yes. The Department's Disciplinary Procedures may be invoked if photos are taken from the phonebook without the consent of the individual in question.

Is the use of the photo compliant with the General Data Protection Regulation (GDPR)?
Yes. Staff images are personal data. Explicit consent is needed to use a photo for any reason other than the staff ID cards. The "opt in" and "opt out" facility on the phone book is the method by which an individual can give or withdraw their consent. These procedures are in line with GDPR.

Appendix Eleven :: Cookies and Website Tracking

Process Id# :: 0008
Process Name :: Website Data Collection & Cookie Policy
Date Last Updated :: 14/8/2020

Description ::

The NSSO gathers statistical and analytical information collected on an aggregate basis of all visitors to our websites / portals. This non-personal data comprises information that cannot be used to identify or contact you, such as:

- Time of visit to websites
- The previous website address from which the visitor reached us, including any search terms used.
- Clickstream data, which shows the traffic of visitors around this website (for example pages accessed and documents downloaded)
- The IP address of a visitor to our websites / portals is recorded as part of this statistical data.

Purpose of Processing ::

No attempt whatsoever is made by the NSSO to link this IP address to any other information that may allow us to identify any individual visiting our websites. The data gathered in aggregate from visitors to our websites helps us to get a better understanding of the areas of interest to our visitors and to better design and organise our websites / portals.

Links ::

The NSSO's websites / portals contains links to other sites. We are not responsible for the privacy standards of other websites. We encourage you to be aware of this when you leave our sites. This privacy statement relates only to the privacy practices in connection with NSSO's own websites.

Cookies ::

Cookies are small pieces of information, stored in simple text files, placed on your computer by a website. Some cookies can be read by the website on your subsequent visits. The information stored in a cookie may relate to your browsing habits on the webpage, or a unique identification number so that the website can 'remember' you on your return visit. Other cookies are deleted when you close your browser and only relate to the working of the website. Generally speaking, cookies do not contain personal information from which you can be identified, unless you have furnished such information to the website. Guidance on Cookies can be found here on the Data Protection Commission website.

Most browsers allow you to turn off cookies or to customise your settings for cookies. To find out how to do this, see the 'Help' menu on your browser. Please note that if you turn off cookies or change your settings, some features may not work correctly.

Cookies & Regulation 5 of the ePrivacy Regulations ::

Regulation 5 of the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011) ('the ePrivacy Regulations') protects the confidentiality of communications.

Regulation 5(3): A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless
(a) the subscriber or user has given his or her consent to that use, and

(b) the subscriber or user has been provided with clear and comprehensive information in accordance with the Data Protection Acts which—
(i) is both prominently displayed and easily accessible, and
(ii) includes, without limitation, the purposes of the processing of the information

Cookies on the NSSO websites ::

In line with Regulation 5(3) we would highlight that Cookies are in a number of places on the NSSO websites.

- When you first visit this website, you will see a message informing you about cookies. Cookies are only set it you select 'Allow all' or if you choose to set preferences and enable the analytical cookie preferences.
- The following Cookies are set on the various site's if consent is granted for cookies.

https://www.nsso.gov.ie/
Google Analytics

- **Cookie Name:** _gat_gtag_UA_85488233_9
  - **Description:** Used to throttle request rate
- **Cookie Name:** _ga
  - **Description:** Used to distinguish users
- **Cookie Name:** _gid
  - **Description:** Used to distinguish users

Language Selection

- **Cookie Name:** qtrans_front_language
  - **Description:** Remembers your language choice and display's site in that language

http://peoplepoint.gov.ie/
Google Analytics

- **Cookie Name:** _gat_gtag_UA_42328974_2
  - **Description:** Used to throttle request rate
- **Cookie Name:** _ga
  - **Description:** Used to distinguish users
- **Cookie Name:** _gid
  - **Description:** Used to distinguish users

Language Selection

- **Cookie Name:** qtrans_front_language
  - **Description:** Remembers your language choice and display's site in that language

https://pssc.gov.ie/
Google Analytics

- **Cookie Name:** _gat_gtag_UA_85488233_26
  - **Description:** Used to throttle request rate
- **Cookie Name:** _ga
  - **Description:** Used to distinguish users
- **Cookie Name:** _gid
  - **Description:** Used to distinguish users

For any further queries please email DPO@nsso.gov.ie

Appendix Eleven :: NSSO Third Party Release Policy

Process Id# :: 0009
Process Name :: NSSO Third Party Release Policy
Date Last Updated :: 1/4/2020

Description ::

Article 28 of the GDPR details the rules a processor works under. A28(3)(a) states a processor ::
'processes the personal data **only** on documented instructions from the controller, …, unless required to do so by Union or **Member State law** to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest'.

Purpose of Process ::

Some third parties, notably An Garda Siochana (AGS), the Welfare Inspectors of The Department of Employment Affairs and Social Protection (DEASP), GSOC and Revenue Inspectors may make requests to access processing records held by the NSSO on behalf of client bodies. They do this based on powers granted to them in their own legislation. This is different to requests from third parties such as pension scheme auditors.

Under Article 28(3)(a) the NSSO is legally obliged to release such data. This process sets out the steps that should be taken when such a request is received to authenticate, adopting the caution applies in other areas such as Article 12(6).

Access & Control ::

The Data Protection Commission (DPC) considers that requests for downloads of CCTV footage made by An Garda Síochána to third parties should be followed up in writing at all times. Using that basis, any requests for any NSSO held data should be ::

- documented on An Garda Síochána headed paper (official request – can be scanned & submitted);
- quote the explicit and specific data fields they require (minimisation);
- should also cite the legal basis for the request;
    - The AGS DPO has confirmed that they have advised Gardai that they should make the request as an Order Pursuant to Section 41(b) of the Data Protection Act 2018.
    - The NSSO DPO feels S41(b) is a vague enabling power and that a further citation under Official Offences legislation would be more appropriate. The NSSO DPO has accepted the argument of AGS that this would disclose the nature of the offence being investigated and has accepted assurances in good faith that their interpretation has been validated by the DPC.
- The headed paper must be signed, or ideally counter signed, by a Garda at the level of Superintendent or above. The equivalent for a request from DEASP (Principal Officer).

This policy remains under review and in all such cases the DPO must be consulted.

Access request to data :: NSSO staff obligations

1) Any requests for personal data from a third party must be sent to the DPO and to the data protection unit.
2) They will assess the nature of the query and liaise directly with the requester and the controller to determine if the data can be released and/or what further steps need to be taken to validate the request.
3) No team in the NSSO is approved to release any data to any third party without the approval of the data protection teams. The DPO/DPU may advise on the preparation of the data if it is anticipated the data will be released subject to minor clarifications.