**(Draft) DATA PROCESSING AGREEMENT**

BETWEEN:

The [name of PSB], a Public Service Body, as defined in [Section 3](http://www.irishstatutebook.ie/eli/2017/act/26/section/3/enacted/en/html#sec3) of the National Shared Services Act 2017 [Number 26 of 2017 (hereinafter to be referred to as: the **“Controller”**),

AND

The National Shared Services Office (NSSO) [The processor], a Public Service Body, (hereinafter to be referred to as: the **“Processor**”),

And in consideration of the sum of €5.00 (five euro only), receipt of which is hereby acknowledged,

HEREBY AGREE AS FOLLOWS:

1. **Subject matter of this Data Processing Agreement**
   1. This Data Processing Agreement applies to the processing of Personal Data, subject to EU Data Protection Law and Irish Data Protection Law provided for in the ‘Memorandum of Understanding’ (MOU) between the Controller and Processor, the ‘Employee Services Management Agreement’ (ESMA) elaborating on the MOU and any future such Service Management Agreements reached between the parties (hereinafter to be referred to as: “the Agreements”).
   2. The term “EU Data Protection Law” or “GDPR” shall mean 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/EC (General Data Protection Regulation).
   3. The term Irish Data Protection Law shall mean the Data Protection Acts 1988 to [2018](http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print.html).
   4. Any capitalised terms not otherwise defined in this Data Processing Agreement shall have the meaning given to them in the Agreements. Except as modified below, the terms of the Agreements shall remain in full force and effect. Other terms used in this Data Processing Agreement that have meanings ascribed to them in the EU Data Protection law, including but not limited to “Processing”, “Personal Data”, “Data Subject”, “Special Categories of Personal Data”, “Data Breach”, “Controller” and “Processor,” shall carry the meanings set forth under EU Data Protection Law.
   5. Insofar as the Processor will be processing Personal Data, subject to EU Data Protection Law and Irish Data Protection Law, on behalf of the Controller in the course of the performance of the Agreements with the Controller, the terms of this Data Processing Agreement shall apply.
   6. In the event of a conflict between any provisions of the Agreements and the provisions of this Data Processing Agreement, the provisions of this Data Processing Agreement shall govern and control. An overview of the categories of Personal Data, the categories of Data Subjects, the nature and purposes for which the Personal Data are currently being processed and an instruction to process in line with these purposes is provided in Annex 2.

* 1. The Data Protection Authority relevant to this Agreement is the Data Protection Commission (DPC), established under the Data Protection Acts 1988 – 2018.

1. **The Controller and the Processor**
   1. Subject to the provisions of the Agreements, to the extent that the Processor’s data processing activities are not adequately described in the Agreements, the Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Processor.
   2. The Processor undertakes to process the Personal Data only as set forth in the Controller’s written instructions (Annex 2) and no Personal Data will be processed unless explicitly instructed by the Controller. Any new processing activities that the Controller wishes the Processor to carry out on its behalf will be by agreement between the parties and will be reflected in updates to Annex 2.
   3. The Processor will only process the Personal Data on the documented instructions of the Controller to the extent that this is required for the provision of the Services. The processing will be executed exclusively within the framework of the Agreements. The processor shall make no decisions regarding the processing of the personal data for other purposes, including decisions regarding the provision thereof to third parties and the storage duration of the data.
   4. The Processor shall refrain from making use of the personal data for any purpose other than as specified by the Controller.
   5. All personal data processed on behalf of the Controller shall remain the property of the Controller and/or the relevant data subjects.
   6. Should the Processor reasonably believe that a specific processing activity beyond the scope of the Controller’s instructions is required to comply with a legal obligation to which the Processor is subject, the Processor shall inform the Controller of that legal obligation and seek approval from the Controller before undertaking such processing.
   7. The Processor shall never process the Personal Data in a manner inconsistent with the Controller’s documented instructions.
   8. The Processor shall immediately notify the Controller if, in its opinion, any instruction infringes the GDPR or other Union or Member State data protection provisions. Such notification will not constitute a general obligation on the part of the Processor to monitor or interpret the laws applicable to the Controller, and such notification will not constitute legal advice to the Controller.
   9. The Parties have entered into the Agreements in order to benefit from the capabilities of the Processor in securing and processing the Personal Data for the purposes set out in Annex 2. The Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this Data Processing Agreement, in particular the Controller’s written instructions.
   10. The Controller warrants that it has all necessary rights to provide the Personal Data to the Processor for the Processing to be performed in relation to the Services, and that one or more lawful bases set forth in EU Data Protection Law and in Irish Data Protection Law support the lawfulness of the Processing. To the extent required by EU Data Protection Law and Irish Data Protection Law, the Controller is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another legal basis set forth in EU Data Protection Law or in Irish Data Protection Law supports the lawfulness of the processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by a Data Subject, the Controller is responsible for communicating the fact of such revocation to the Processor, and the Processor remains responsible for implementing Controller’s instruction with respect to the processing of that Personal Data.
2. **Confidentiality**
   1. Without prejudice to any existing contractual arrangements between the Parties, the Processor shall treat all Personal Data as confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.
3. **Security**
   1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include, at a minimum, the security measures agreed upon by the Parties in Annex 3.
   2. Both the Controller and the Processor shall maintain written security policies that are fully implemented and applicable to the processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the Personal Data, conducting appropriate background checks, requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the Processing.
   3. At the request of the Controller, the Processor shall demonstrate the measures it has taken pursuant to this section and shall allow the Controller to audit and test such measures.
   4. Unless otherwise required by a Supervisory Authority of competent jurisdiction, the Controller shall be entitled on giving at least 30 days’ notice to the Processor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Processor, audits of the Processor´s premises and operations to the extent needed to confirm compliance with the terms of this agreement as they relate to the protection of Personal Data.
   5. The Processor shall cooperate with such audits carried out by or on behalf of the Controller and shall grant the Controller´s auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Processor shall provide the Controller and/or the Controller´s auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Controller to ascertain the Processor´s compliance with this Data Processing Agreement, and/or to ascertain the Processor’s compliance with any approved code of conduct or approved certification mechanism referenced in Section 4.4.
   6. The Processor’s adherence to either an approved code of conduct or to an approved certification mechanism recognized under EU Data Protection Law or Irish Data Protection Law may be used as an element by which the Processor may demonstrate compliance with the requirements set out in Section 4.1, provided that the requirements contained in Annex 3 are also addressed by such code of conduct or certification mechanism.
   7. It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the personal data, as set out in the Agreements.
   8. Notwithstanding the requirements set out in Section 4.7 of this Agreement, it is the responsibility of each Party to ensure that its staff members are appropriately trained in the requirements as set out in EU Data Protection Law and Irish Data Protection Law.
   9. The level, content and regularity of training referred to in Section 4.8 shall be proportionate to the staff member’s role, responsibility and frequency with respect to their handling and processing of personal data.
4. **Improvements to Security**
   1. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore evaluate the measures as implemented in accordance with Section 4 on an on-going basis in order to maintain compliance with the requirements set out in Section 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in EU Data Protection Law, Irish Data Protection Law or by data protection authorities of competent jurisdiction.
   2. Where an amendment to the Agreements is necessary in order to execute a Controller instruction to the Processor to improve security measures as may be required by changes in EU Data Protection Law or Irish Data Protection Law from time to time, the Parties shall negotiate an amendment to the Agreements in good faith.
5. **Data Transfers** 
   1. The Processor shall promptly notify the Controller of any planned permanent or temporary transfers of Personal Data to a third country, including a country outside of the European Economic Area without an adequate level of protection, and shall only perform such a transfer after obtaining authorisation from the Controller, which may be refused at its own discretion. Annex 4 provides a list of transfers for which the Controller grants its authorisation upon the conclusion of this Data Processing Agreement.
   2. To the extent that the Controller or the Processor are relying on a specific statutory mechanism to normalise international data transfers and that mechanism is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Controller and the Processor agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.
6. **Information Obligations and Incident Management**
   1. When the Processor becomes aware of an incident that has a material impact on the Processing of the Personal Data that is the subject of the Agreements, it shall promptly notify the Controller about the incident, shall at all times cooperate with the Controller, and shall follow the Controller’s instructions with regard to such incidents, in order to enable the Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.
   2. When the Processor becomes aware of a “breach incident” that has a material impact on the Processing of the Personal Data that is the subject of the Agreements, it shall implement the agreed breach exploration process outlined in process 0000 of Annex 2.
   3. The term “incident” used in Section 7.1 shall be understood to mean in any case:
7. a complaint or a request with respect to the exercise of a Data Subject’s rights under EU Data Protection Law;
8. an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;
9. where, in the opinion of the Processor, implementing an instruction received from the Controller would violate applicable laws to which the Controller or the Processor are subject.
   1. The terms “breach incident” used in Section 7.2 shall be understood to mean in any case:
10. any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;
11. any breach of the security and/or confidentiality as set out in Sections 3 and 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;
    1. The Processor shall at all times have in place written procedures which enable it to promptly respond to the Controller about an incident or a breach incident. Where the breach incident is reasonably likely to require a data breach notification under EU Data Protection Law or Irish Data Protection Law, the Processor shall implement its written procedures without undue delay after the Processor becomes aware of such an incident.
    2. Any notifications made to the Controller pursuant to Section 7.1 shall be addressed to the employee of the Controller, who should be the Data Protection Officer or Compliance Officer and whose contact details are provided in Annex 1 of this Data Processing Agreement and, in order to assist the Controller in fulfilling its obligations under EU Data Protection Law or Irish Data Protection Law, should contain:
12. a description of the nature of the incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
13. the name and contact details of the Processor’s Data Protection Officer or another contact point where more information can be obtained;
14. a description of the likely consequences of the incident; and
15. a description of the measures taken or proposed to be taken by the Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.
16. **Contracting with Sub-Processors**
    1. The Processor shall not subcontract any of its Service-related activities consisting (partly) of the processing of the Personal Data or requiring Personal Data to be processed by any third party without the prior written authorisation of the Controller.
    2. The Controller authorises the Processor to engage the sub-processors listed in Annex 6 for the service-related Data Processing activities described in Annex 2. Processor shall inform the Controller of any addition or replacement of such sub-processors, giving the Controller an opportunity to object to such changes.
    3. If the Controller sends the Processor a timely written objection notice, setting forth a reasonable basis for objection, the Processor will make a good-faith effort to resolve Controller’s objection. In the absence of a resolution, the Processor will make commercially reasonable efforts to provide Controller with the same level of service described in the Agreements, without using the sub-processor to process Data Controller’s Personal Data. If the Processor’s efforts are not successful within a reasonable time, each Party may terminate the portion of the service which cannot be provided without the sub-processor, and the Controller will be entitled to a pro-rated refund of the applicable service fees.
    4. Notwithstanding any authorisation by the Controller within the meaning of the preceding paragraph, the Processor shall remain fully liable vis-à-vis the Controller for the performance of any such sub-processor that fails to fulfil its data protection obligations.
    5. The Processor shall ensure that the sub-processor is bound by data protection obligations compatible with those of the Processor under this Data Processing Agreement, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU Data Protection Law and Irish Data Protection Law.
    6. The Controller may request that the Processor audit a Third Party Sub-processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Controller in obtaining a third-party audit report concerning the Third Party Sub-processor’s operations) to ensure compliance with its obligations imposed by the Processor in conformity with this Agreement.
17. **Returning or Destruction of Personal Data**
    1. Upon termination of this Data Processing Agreement, upon the Controller’s written request, or upon fulfilment of all purposes agreed in the context of the Services whereby no further processing is required, the Processor shall, at the discretion of the Controller, either delete, destroy or return all Personal Data to the Controller and destroy or return any existing copies.
    2. The Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Controller, at the discretion of the Controller.
    3. The Processor shall not retain or process personal data for longer than is necessary to carry out the agreed purposes as agreed within the Agreements, or for longer than any period set by the Controller. For the avoidance of doubt, the Controller reserves the right to determine the periods for which the Processor may retain the personal data processed under the Agreements.
    4. On the instructions of the Controller, the Processor shall ensure that all personal data processed, as defined by the Agreements, is returned to the Controller or destroyed in accordance with the Controller’s instructions. The Controller reserves the right to issue instructions to the Processor under this Section at any time.
    5. The Controller reserves the right to issue instructions to the Processor as to the methods by which personal data is destroyed under Sections 9.1 and 9.2.
    6. Following the deletion of personal data under Sections 9.1 and 9.2, the Processor shall notify the Controller that the personal data in question has been deleted. Where applicable, the Processor shall also provide confirmation that the personal data has been destroyed in accordance with any instructions issued by the Controller under Section 9.4.
18. **Assistance to Data Controller**
    1. The Processor shall assist the Controller, by way of appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller’s obligation to respond to requests for exercising the Data Subject’s rights under the EU Data Protection Law and Irish Data Protection Law.
    2. Taking into account the nature of processing and the information available to the Processor, the Processor shall assist the Controller in ensuring compliance with obligations pursuant to Section 4 (Security), as well as other Controller obligations under EU Data Protection Law and Irish Data Protection Law that are relevant to the Data Processing described in Annex 2, including notifications to a supervisory authority or to Data Subjects, the process of undertaking a Data Protection Impact Assessment, and with prior consultations with supervisory authorities.
    3. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the Processor’s obligations and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.
19. **Duration and Termination**
    1. This Data Processing Agreement shall come into effect on the effective date of the Memorandum of Understanding.
    2. Termination or expiration of this Data Processing Agreement shall not discharge the Processor from its confidentiality obligations pursuant to Section 3.
    3. The Processor shall process Personal Data until the date of expiration or termination of the Agreements, unless instructed otherwise by the Controller, or until such data is returned or destroyed on instruction of the Controller.
    4. The Processor, in line with the provisions of the Memorandum of Understanding, is authorised by the Controller to respond directly to requests for information from the Comptroller and Auditor General, the Public Accounts Committee and other Oireachtas Committees as required.
20. **Miscellaneous**
    1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Agreements, the provisions of this Data Processing Agreement shall prevail.
    2. This Data Processing Agreement is governed by the laws of Ireland. Any disputes arising from or in connection with this Data Processing Agreement shall be brought exclusively before the competent court.
    3. Where a data subject notifies the Processor that they wish to exercise their rights under Articles 15 to 22 of the GDPR, the Processor will advise the data subject to engage with the Controller. The Processor will assist the controller in giving data subjects access to their rights, for example providing relevant information to the Controller for Subject Access Requests. For the purpose of clarity, while this includes requests under Article 16 for the rectification of inaccurate data, the Controller authorises the Processor to update basic contact and banking information necessary for the performance of processing.
    4. The Processor will publish a ‘[Data Protection Policy](https://www.nsso.gov.ie/corporate-2/data-protection/)’ which provides additional information to data subjects and Controllers on the data protection policies in place.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed

for and on behalf of the Controller

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed

for and on behalf of the Processor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:

**Annex 1 ::**

**Contact details of both Data Protection Officers**

Contact information of the Data Protection Officer of the Controller.

**<name>**

Data Protection Officer

Phone:

Email: [dpo@xxxxx](mailto:dpo@opw.ie)

Contact information of the Data Protection Officer of the Processor.

**Adam Egan**

Data Protection Officer

Assistant Principal

National Shared Services Office

5, Belfield Office Park,

Beech Hill Road,

D04 A9P2

Phone: 086 701 3294

Email: dpo@nsso.gov.ie

**Annex 2 ::**

**List of Processes to be carried out with instruction to process.**

The following is the list of processes which the NSSO carries out. The Controller instructs the Processor to carry out these processes on its behalf in line with [Schedule 2](http://www.irishstatutebook.ie/eli/2017/act/26/schedule/2/enacted/en/html#sched2), Section 9 of the National Shared Services Office Act 2017 and [S.I. No. 267](http://www.irishstatutebook.ie/eli/2018/si/267/made/en/print) of 2018. Processing on behalf of the Controller will continue for the duration of the term defined by the Agreements or until otherwise notified in writing by the Controller.

It includes some internal NSSO policies which are listed to provide assurances to the controller that said controls are in place.

The Processor will not process personal data on behalf of the Controller other than in accordance with the National Shared Services Office Act 2017 and the Agreements. The Processor will maintain a Record of all Processing Activities in accordance with Article 30 of the GDPR. An index of agreed processes follows ::

**Note text to be removed at signing :: This is understood to be a comprehensive list of processing carried out by the NSSO. The purpose of this initial draft Annex 2 is to regularise existing processes being carried out for bodies.**

**There may be several processes that do not apply to your organisation. Where you identify processes that do not apply to your organisation or if you identify any processes that should be on this list, then the NSSO will amend the list of processes in agreement with you. Future updates to Annex 2 will be agreed via Service Management Agreements or other agreed mechanisms.**

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| **No#** | **Process Name** | **Last Updated** | **Section** |
| **NSSO Administration Processes :: 0000 - 0999** | | | |
| **Data & Quality Compliance** | | | |
| 0000 | NSSO Client Breach Reporting Process | 1/7/2019 | IGT |
| 0001 | Subject Access Request (SAR) - from Client PSBs | 1/7/2019 | IGT |
|  | etc |  |  |
|  | etc |  |  |
|  |  |  |  |
|  |  |  |  |
| **HRSS Processes on behalf of a PSB :: 1000 - 1999** | | | |
| **As per Article 3 of S.I. 267 of 2018 and Schedule 2 of the NSSO Act 2017.** | | | |
| **No#** | **Process Name :: 1000 - 1999** | **Last Updated** | **Section** |
| **Staff Set Up process** | | | |
| **Organisation Structure (OSM) - New hires, grade relationships)** | | | |
| 1001 | Secondment | 1/1/2019 | OSM |
| 1002 | Acting Up | 1/1/2019 | OSM |
| 1003 | Authorisation List | 1/1/2019 | OSM |
| 1004 | Employee Class Change | 1/1/2019 | OSM |
|  | etc |  |  |
|  | etc |  |  |
|  |  |  |  |
|  |  |  |  |
| **Pay (PSSC) Processes on behalf of a PSB :: 2000 - 2999** | | | |
| **No#** | **Process Name** | **Last Updated** | **Section** |
| **Payroll Process** | | | |
| **Payroll Amendments** | | | |
| 2009 | Pay Awards- Pay Increases and Adjustments | 1/1/2019 | Payroll |
| 2010 | Maternity/Adoption Leave Unpaid | 1/1/2019 | Payroll |
| 2011 | Maternity/Adoption Leave Paid | 1/1/2019 | Payroll |
| 2012 | Parental Leave | 1/1/2019 | Payroll |
| 2424 | Special arrangement currently in place in respect of DFA – additional approval checking process | 1/1/2019 | Expenses |
|  | etc |  |  |
|  | etc |  |  |
|  |  |  |  |

**Annex 3: Security Measures**

Processor shall:

1. ensure that the Personal Data can be accessed only by authorised personnel for the purposes set forth in Annex 2 of this Data Processing Agreement;
2. take all reasonable measures to prevent unauthorised access to the Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;
3. build in system and audit trails;
4. use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;
5. account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of Personal Data;
6. ensure pseudonymisation and/or encryption of Personal Data, where appropriate;
7. maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
8. maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
9. implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data;
10. monitor compliance on an ongoing basis;
11. implement measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Controller;
12. provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

**Annex 4 ::**

**Transfers to sub-processors outside of the EEA**

Transfers to sub-processors in third countries, including countries outside the European Economic Area without an adequate level of protection for which the Controller has granted its authorisation:

|  |  |
| --- | --- |
| **Sub-processor Name** | **Country** |
| None | N/A |

The NSSO does not use cloud based back—ups and no such services are located outside the EEA.

Note :: We have no sub-processing taking place in the United Kingdom and thus no potential Brexit related exposures

**Annex 5 ::**

**Breach Reporting Process**

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 34 of the GDPR.

The controller therefore authorises the processor to notify the Data Protection Commission, in line with the process agreed with in process 0000 in Annex 2, of any breaches of data caused by the NSSO on the condition that the notification process is carried out in accordance with Article 33 and 34 of the GDPR.

The processor 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 34 of the GDPR.

This removes the need for the controller to contact the Data Protection Commissions about breaches it is notified about, though the controller retain the right to contact the Commission should it so desire.

The current version of process 0000, dated November 12th 2019, follows for your convenience.

**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)**

1. 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 -
   1. risk or no risk,
   2. If there is a risk then to set which level of risk should apply.
2. 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.
3. 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.
4. The NSSO DPO will consult with the team and others as appropriate to finalise the wording of the breach notification form.
5. 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.
6. 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**

1. Breach notifications had issued to [breaches@dataprotection.ie](mailto: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.
2. The DPC will reply shortly with a receipt and breach code, eg BN—18-7-621.
3. Document this in your records and ensure the NSSO DPO is forwarded the notification email.
4. Any correspondence with the DPC must issue from [dataprotection@pssc.gov.ie](mailto:dataprotection@pssc.gov.ie), [dataprotection@peoplepoint.ie](mailto:dataprotection@peoplepoint.ie), or [dataprotection.finance@nsso.gov.ie](mailto:dataprotection.finance@nsso.gov.ie) it is not to issue from personal email addresses.
5. You should always cc [dpo@nsso.gov.ie](mailto:dpo@nsso.gov.ie) on all DPC emails.
6. 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**

1. All breaches irrespective of risk must be notified to the controller PSBs.
2. 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.
3. 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.
4. 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**

1. 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)](https://gdpr-info.eu/art-34-gdpr/).
2. 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).
3. 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

**Annex 6 ::**

**Third Party Service Providers**

|  |  |
| --- | --- |
| **System/Service** | **Entity** |
| Common Office IT services  (PC’s/Laptops, Comms, Phones, Office Software etc) | Office of the Government Chief Information Officer (OGCIO) |
| HRMS Application Support | Bearingpoint |
| Payroll Application Support | Core |
| FMS Application Support | Accenture |
| Data analytics on the Core platform for reporting | MakoData |
| HRMS Infrastructure Service and Administration | OGCIO |
| Payroll Infrastructure Service and Administration | Department of Agriculture and the Marine / Department of Education |
| FMS Infrastructure Service and Administration | Accenture |
| Interactive Voice Response | Vodafone, Vocalcom. |
| Document Management | Storm |
| Internal engagement analytics | Poppulo |
| ISAE Audit assessments | Mazars |
|  |  |