APPENDIX A

Data Protection Measures in place in NSSO Operations October 2015

- A **Data Protection Policy for Shared Services** (March 2014) is in place.

- Each operation has a fully trained Data Protection Compliance Officer (DPCO) in place. The DPCO is supported by the Operations Governance Manager in NSSO. Compliance officers are ready to respond to any breach of security swiftly and effectively.

- All staff in operations receive data protection training at induction, and refresher training on an annual basis.

- **Reporting of data breaches** within operations is managed through the DPCO who gathers the data on the breach. Each breach is treated with the utmost seriousness. A breach is investigated, reported and assessed through a root cause analysis approach. Individuals who cause a data breach are spoken with and further training is provided as required. A process in in place in each operation to report breaches to the Office of the Data Protection Commissioner, the Customer Department Data Controller, the data subjects as appropriate under the guidance of the Customer Department Data Controller, D/PER Data Controller and the Department of Social Protection.

- A **Records and Retention Management Policy** is currently being drafted for the NSSO. This Policy, when completed, will identify records and information which are managed, stored, retained, destroyed or transferred, if appropriate, to an off-site location. The Policy will also specify the minimum requirements for the retention and disposal of departmental records and information, held in all formats (electronic and physical). This Policy will assist the NSSO and its Customer Departments in identifying what records are held in each of its Shared Service Centres and where they are physically, electronically located. Appropriate and suitable technical security measures, and organisational measures, will be put in place to support this Policy.

- A **National Shared Services Office Protocol** is in place for the retention of information by external audit firms **as part of the ISAE3402 Audit process** to meet external audit requirements and to protect personal data in Shared Services Centres.

- A **Civil Service Telephone and Call Recording Policy** (July 2014) is in place to ensure that the use of recordings is fair and compliant with the relevant legislation.

- An **annual data security audit** is undertaken by the DPCO in each operation – the first will take place in Q4 2015.

- A **breach of the Data Protection Act on the part of PeoplePoint was identified on the 16th October last**. Personal data of some 317 civil servants who had incurred an overpayment of salary was shared with Local HR sections of 22 customer departments as a result of human error. The following process was followed:

  - The error was immediately identified and all of the recipients were immediately asked to delete the information and confirm that it was not circulated any further.
  - The Office of the Data Protection Commissioner was properly notified of the data breach as per PeoplePoint process.

    - Each of the relevant data controllers, and the individuals affected were also notified of the breach.

- The Office of the Data Protection Commissioner has indicated that it is satisfied with the actions taken by PeoplePoint to date, and has concluded its file on this matter. Furthermore, it has stated that it expects that "PeoplePoint will introduce new procedures to reduce the risk of a similar incident recurring". The process is currently under review.
- To date, PeoplePoint has received contact, by email or telephone, from 49 of the affected individuals. These queries are being handled by a dedicated data protection section, as per PeoplePoint process.