INPDR Personal Data Security Policy

File name: INPDR Personal Data Security Policy

	Name	Title	Signature	Date
Author	Conan Donnelly	Registry Manager		6th March 2020
Reviewer				
Authoriser				

Effective Date	6th March 2020
Review Date	

Version	Date	Author	Changes
0.1	6th March 2020	Conan Donnelly	

INPDR Personal Data Security Policy

Introduction to Personal Data Security and the obligations and requirements of INPDR:

INPDR, like all data controllers, has a positive legal obligation to secure the Personal Data it processes. The General Data Protection Regulation provide that:

"you must comply with, and demonstrate compliance with, all the data protection principles as well as the other GDPR requirements. You are also responsible for the compliance of your processor(s)"

In deciding on the specific measures to be adopted, the controller may have regard to the state of the technological art and the costs involved, whilst ensuring an appropriate level of security, having regard to the possible harm that might result from a failure to secure the data and the nature of the data. For example, stricter controls would be warranted over access to sensitive personal data or financial information.

Apart from the risk of harm to data subjects, or enforcement action and substantial financial penalties for non-compliance, other risks to INPDR arising from failures to secure personal data include:

- Inability of INPDR to perform its functions
- Damage to INPDR'S reputation and loss of public trust;
- Loss of trust of INPDR staff, where their personal data is affected;
- Costs involved in dealing with serious data breaches;
- Possible civil actions for damages by the persons affected by a failure to secure data.

Guidelines:

1. **Portable computers, removable media and mobile phones**

   The ICO Guidance highlights that laptops, USB sticks, backup media like tapes or CDs, mobile phones, etc, are all particularly at risk from theft or accidental loss.

Where they are, or may be, used to store personal data they should be encrypted. Whole device encryption should be applied. Backup copies of production IT systems data should be encrypted as they are being made.

Only INPDR-owned devices should be used to access INPDR IT systems such as email. Automatic locking and pass codes should be applied to mobile phones which may access such services or otherwise be used to store personal data.

The personally-owned equipment of staff should never be used to access or store personal data which INPDR processes.

Use should, where possible, be made of services to remotely locate and/or erase portable computing devices and mobile phones.

2. Clean Desk

Files and documents should not be left unsecured on or around desks. At a minimum, papers should be securely stored at the end of each working day in a locked cabinet. Depending on the nature of the data, it may be appropriate to secure documents when staff are away from their desks at meeting, on breaks, etc.

Shredding consoles should be conveniently located for the use of all staff, to avoid the risk that personal data might be placed with ordinary waste.

3. Access Controls

Staff should only have access to the personal data they need to carry out their duties. Appropriate access controls should be applied to ensure this is the case.

Desktop PCs, etc, should automatically lock after an appropriate period of inactivity and require password authentication to unlock.

Password policies should require staff to use and regularly change robust passwords or passphrases. Other appropriate access methods may be deployed, such as swipe cards or biometric controls (although these can in themselves introduce further personal data protection risks).

Appropriate measures should be taken to prevent the bulk downloading of data from INPDR systems, for example, by restricting the use of USB ports.

4. Logs and Audit Trails

It may not always be possible to predict in advance the data a given staff member may need to access. Appropriate measures should be applied to log the identity of person accessing and editing data, giving dates and times. Staff should be advised that their accesses are being monitored and that they may be required to justify their access to records on the basis of their current work assignments.

Such access logs may also be used help identify unauthorised access to systems by intruders.

5. Technological security measures and issues

Data protection act require appropriate technological measures to be taken to secure personal data. A full examination of these is beyond the scope of this document and should be addressed in INPDR'S Information Security policy, but some of the areas to be covered would include:

- **Wireless network security**
- **Encryption standards**
- **Anti-virus software**
- **Firewalls**
- **Remote access to systems**
- **Software updates**
- **Access controls**

6. Backups

We often think of personal data security as relating to the prevention of unauthorised access. However, it is equally important to stop unauthorised or accidental alteration or destruction of personal data.

As part of INPDR'S Business Continuity Plans, appropriate account should be taken of these requirements. The backup procedures should also require the encryption of backups as they are made, so that a loss of backup media will not result in a personal data breach.

7. End-of-life equipment (PCs, Compact Discs, Hard Disc Drives, External Storage devices, USB memory sticks, etc.)

These will be securely disposed of in accordance with INPDR'S Personal Data Retention Policy.

8. Physical security

These measures should include consideration of:

- Perimeter security;
- Access to sensitive areas such as server rooms;
- Location of computer equipment;
- Location of file storage;
- Secure destruction of paper files and computer media & equipment.
- Home working policies.

9. Staff awareness

Experience and surveys repeatedly show that the greatest risk of a serious data protection incident arises from the inappropriate handling of personal data by staff, as opposed for example, to the risks from "hacking". In the great majority of cases, these stem not from malice, but from staff either unintentionally disclosing data (say, emailing to the wrong address), or intentionally disclosing data to someone who is not authorised to receive it.

The Data Protection Officer should ensure that staff who handle personal data receive training in their obligations and INPDR'S appropriate to the nature and amount of data handled, and the level of their responsibility. Staff should also be required to read the

relevant sections of INPDR'S data protection policies and confirm that they understand and will adhere to them.

Refresher training and/or reminders of policies and obligations should be provided at reasonable intervals.

Related Policies:

- INPDR Data Protection Policy
- INPDR Information Security Policies
- INPDR Business Continuity Plan
- INPDR Data Subject Rights Policy
- INPDR Personal Data Breach Management Policy
- INPDR Personal Data Breach Incident Log
- INPDR Personal Data Retention Policy

Definitions

"Data Subject" means a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

End of document