Guide to preparing and using the NUIG Personal Data Security Schedule (PDSS)

Introduction

The use and processing of personal data is regulated by both EU and Irish legislation. As the legislation is both extensive and complex the purpose of the PDSS (Personal Data Security Schedule) is to assist members of staff, researchers and others in meeting their legal obligations when interacting with, or processing, personal data in any way for which NUIG is ultimately responsible. The PDSS is intended to be unit or project team specific i.e. the categories of personal data listed are the categories relevant to the unit / research team.

Purpose

The purpose of this guide is to assist Heads of Units and Principal Investigators in compiling a unit specific PDSS. Once finalized the PDSS is to be distributed and made available to all unit staff and project team members. The importance of following the PDSS, and its implications, should be emphasized when bringing it to the attention of staff and team members.

Definition of 'Personal Data'

Personal data is data relating to a living individual (i.e. the 'Data Subject') who is, or can be, identified either from the data itself or from the data in conjunction with other information that is in, or is likely to come into, the possession of the 'Data Controller' (i.e. NUIG and its constituent units e.g. faculties, schools, support offices, campus companies, research centres, research teams etc.). It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Examples of some typical categories of personal data known to exist within the NUIG community are listed in the appendix to this guide. Heads of Unit / Principal Investigators should consider whether their unit or team processes any of the categories of personal data listed.

Please note that:

- the definitions of 'personal data' and 'processing' are deliberately very broad;
- the list in the appendix is not exhaustive - your unit or team may process other categories of personal data which are not listed in the appendix; &
- personal data can be held and/or processed in either an electronic and/or paper format or indeed both.

Definition of 'Sensitive Personal Data'

Due to its nature sensitive personal data requires a higher level of security and more robust management. Sensitive personal data is data that relates to an individual's:

(a) racial or ethnic origin;
(b) political opinions;
(c) physical or mental health or condition;
(d) membership of a trade union;
(e) sexual life or orientation;
(f) commission or alleged commission of any offence;
(g) religious beliefs or similar; &
(h) genetic or biometric information.

Completing a PDSS for the unit or team

The Head of Unit / Principal Investigator should discuss with their staff the types of personal data which already exist, or are likely to come into, the unit or team. An initial attempt should then be made to fill in as many of the panels as possible in the draft PDSS template supplied with this guide. The University Data Protection Officer will assist with any queries you may have.

Explanation of PDSS Panels

Panel 1 - Reference number
Insert as many rows as required to list all the various categories of personal data processed by the unit or team.

Panel 2 - Type, category or description of the personal data
State the type of personal data e.g. staff CVs / student stipend file /patient history etc. (see appendix). It is best to be specific and precise, especially if there are a number of fundamentally different sub-categories of personal data.

Panel 3 - Normal or 'sensitive' personal data
State whether the personal data is 'normal' or 'sensitive'. Note that sensitive personal data requires a higher degree of control / security measures and these should be documented in panel 11 – 'Safeguards and Controls'.

Panel 4 - Format of the data (Electronic / Paper / Both)
State here the format in which the data is held or processed by the unit or team. This will assist with deciding on the type and nature of safeguards and security controls to be applied to the data.

Panel 5 - Unit's or Team's reason or purpose for processing the data
State here why the data was originally obtained e.g. for HR administration, medical research, processing payments from staff/students/customers etc. The purpose must be related to the unit or team's activity or role. Personal data is not to be obtained and/or processed without a good business case or reason for doing so.

Panel 6 - Legal basis for processing the data
Under the law personal data may only be processed provided there is a legal basis for doing so. There are six legal bases for processing personal data as listed below. Select the one which applies best to each category of personal data listed on the PDSS. If you are unsure then leave the panel blank and discuss the issue with the University Data Protection Officer.

a) **Consent (e.g. the majority of student personal data)**
Where consent is used as a basis it must be freely given, informed and unambiguous. This will require that a written Data Protection Notice is brought to the attention of the Data Subject. The consent must be specific to the purpose for which the data has been collected. The age of consent to processing is 16. Consent can be implicit, but if there is sensitive personal data involved the consent must be explicit (i.e. written or alternatively that a consent box is ticked). In the most cases where a NUIG registered student's data is being processed their consent will have been obtained by virtue of registering as a student in each academic year. Note that this basis will generally not apply to the personal data of employees. One of the other bases for processing will have to be found in such cases.

b) **Legitimate interest (e.g. for health and safety reasons)**
Organisations have a legitimate interest to protect their business and this is a lawful basis for processing personal data. However the data must be processed for specific and legitimate purposes that are proportionate and necessary. The assessment of whether this basis can be applied will be conducted on a case-by-case basis after balancing the rights of all the stakeholders.

c) **Fulfilment of a contract (e.g. often applies in research projects carried out by NUIG for a 3rd party)**
If the individual who owns the personal data has signed a contract with either NUIG or a 3rd party which requires the processing of their personal data then this qualifies as a basis for processing.

d) **Statutory obligation (e.g. tax law compliance, Garda Vetting, HEA returns etc.)**
If NUIG is required by legislation to process a particular category of personal data then that qualifies as a basis for processing.

e) **Vital or emergency situation (e.g. hospital asking for details of next of kin of staff or students)**
If an individual's health and wellbeing requires the urgent processing of their personal data then that qualifies as a basis for processing.

f) **Public interest (e.g. may relate to some research projects related to public health)**
Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

Panel 7 - Responsibility for the security of the data
Insert here the title of the primary person within the unit or team who is charged with responsibility for the security of the personal data. This person will ensure that the PDSS is adhered to and communicated regularly to all unit or team members.

Panel 8 - Who may access the data?
Access to personal data must be controlled, especially so if the data is sensitive. Only individuals with a legitimate business interest in the data are to be allowed access to it. The Head of Unit or the project team Principal Investigator must decide at the outset to whom access will be granted.

Panel 9 - Who may amend the data?

One of the principles of data protection law is that the data must be safeguarded from accidental erasure or amendment. Accordingly only designated persons should have the authority to amend the data. In most cases this right will be restricted to unit staff or team members only. Where the data may be amended by others they should only be permitted to do so after an assessment of the necessity for allowing them that right.

Panel 10 - With whom may the data be shared?
Access to personal data, as noted above in panel # 8, is to be restricted. However the Head of Unit or the Principal Investigator may allow the sharing of the data to other NUIG units or an external 3rd party. The authorised units/parties are to be listed in this panel. Note that where NUIG is using an external 3rd party to process the data in any way a Data Processing Agreement may be necessary. Please contact the University Data Protection Officer if this is the case.

Panel 11 - Safeguards and controls to be applied to the data by Unit staff / Research team
Use this panel to list all the measures (controls, protocols, procedures, practices, data processing contracts etc.) in place to safeguard the data while it is within the control of the unit or team. The type and level of security applied will be dependent upon the nature of the data, its format and its sensitivity. Examples of typical controls for electronic records would be (a) a valid staff login is necessary to access the record (b) password protection (c) prohibition on the transfer of data using USB keys (d) laptops/hard drives are to be encrypted (e) the establishment of a hierarchy of access rights etc.

Panel 12 - How long is the data to be held / retained?
Personal data must only be retained for so long as there is a justifiable business reason for doing so. With very few exceptions personal data may not be retained indefinitely. It is up to the unit or research team to establish an upper retention limit for each category of personal data under its control. At the end of the retention period the data must be either erased or destroyed or anonymized or, alternatively, returned to the owner of the data or to the Data Controller where NUIG is acting as a Data Processor.

Panel 13 - Responsibility for the panel 12 task is assigned to?
Insert here the title of the primary person charged with responsibility for the security of the data in the unit or research project / team. That person will ensure that once the data has reached the end of its retention period, as stated in panel 12, that the required action will be carried out i.e. its erasure, destruction, anonymization or return to owner.

Panel 14 - Method of disposal for the data
Personal data must be disposed of in a safe and secure manner at the end of its retention period. State here how this is to be achieved. If the data is stored in a:

a) paper based format then shredding or disposal via a secure bin is recommended; or
b) if it is stored in an electronic based format then deletion of the record or full anonymization of the data is recommended.

Panel 15 - Is the data shared outside of NUIG?
Please state 'Yes' or 'No' as appropriate. If yes, state with whom and why. A formal Data Processing Agreement may be required where a 3rd party processes the data on behalf of a NUIG unit or project team. If there is any doubt you should contact the University Data Protection Officer.

Panel 16 - Any other comments?
Fill in this panel with any other comments relevant to the category of personal data.

Using the PDSS

The PDSS is intended to assist both NUIG management and staff with applying good personal data practices. It is to be kept up to date and shared with unit staff or project team members on a regular basis. A copy of the finalized PDSS will also be maintained by the University Data Protection Office.

Appendix: Examples of some typical categories of personal data which may exist within NUIG units or research project teams

1) Personnel files (paper or electronic) containing names, CVs, references, staff request forms, copies of employment contracts, PPS numbers, passport photos, contact details, salary, qualifications, contract status, contract start/end dates etc.
2) Bank account details (e.g. Wages Payment Form).
3) Expense claims.
4) Online identifiers (such as an IP address).
5) Location data.
6) Documentation relating to the Garda National Immigration Bureau.
7) Reports to funders with details of staff member's qualifications, rates of pay, contract duration etc.
8) Medical certs / Doctor sick notes.
9) Annual leave records.
10) Sabbatical leave records.
11) CCTV images / Video capture images / Voice recordings.
12) Researcher Hosting Agreements.
13) Continuing professional development records.
14) Research student stipend documentation.
15) Research student progress forms – PGR2.
16) Scholarship Application Forms – SAF.
17) Analysis of staff workload records.
18) Staff / student performance review documentation.
19) Questionnaires obtained from research subjects (paper/on-line).
20) Research subject consent forms.
21) Contact lists or mailing lists for students, research subjects and research partners.
22) Student exam results / broadsheets.
23) Student Module exemptions.
24) CV's of tutors.
25) Plagiarism notifications and related documentation.
26) Correspondence with students.
27) Postponement / deferral documentation / Extenuating circumstances forms for students.

28) References for staff / students.
29) Feedback forms.
30) Assignment results.
31) Garda Vetting documentation for students and members of staff.
32) Job offer notices.
33) Travel grant application forms.
34) Exam validation reports for all students per modules.
35) Clinical files relating to students
36) Clinical files relating to research participants.
37) Recordings taken using mobile or personal cameras e.g. 'Lifelogging'.
38) Profiles of researchers / students / other individuals held in any format.
39) Micro-Teaching digital recordings and any related material (i.e. Parental Consent Forms).
40) Customer credit card or ATM card details.
41) Bank details of suppliers who are individuals (i.e. not legal entities such as companies, trusts).
42) Alumni details.
43) Agent details (contact addresses, bank account details etc.).

End.