

These guidelines were prepared for DSP staff and some references may not apply. Any queries should be referred to the DSP Divisional Contract Manager

Contents

1. DSP Data Protection Guidelines
2. DSP Data Protection Policy
3. DSP Guidance Note for Staff Disclosure of Personal Data

DATA PROTECTION ACTS 1988 AND 2003

Data Protection Guidelines

1. Purpose of these Guidelines

The purpose of these Guidelines and Procedures is to assist staff in supporting the Department's **Data Protection Policy**, which affirms its commitment to protect the privacy rights of individuals in accordance with the legislation. These Guidelines should be read in conjunction with the Department's **Acceptable Use Policy** and the **Email and Internet Policy**.

2. What are the Data Protection Acts, 1988 and 2003?

The Data Protection Acts 1988 and 2003 are designed to protect an individual's privacy. The Acts confer rights on individuals in relation to the privacy of their personal data as well as responsibilities on those persons holding and processing such data. In particular, they provide for the collection and use of data in a responsible way, while providing protection against unwanted or harmful uses of the data.

All staff should familiarise themselves with the provisions of the Acts. Further information is available on the website of the Office of the Data Protection Commissioner www.dataprotection.ie.

3. Department's Obligations

There are Eight Rules of Data Protection which govern the processing of personal data: -

1. Obtain and process the information fairly;
2. Keep it only for one or more specified and lawful purposes;
3. Process it only in ways compatible with the purposes for which it was given to you initially;
4. Keep it safe and secure;
5. Keep it accurate and up-to-date;
6. Ensure that it is adequate, relevant and not excessive;
7. Retain it no longer than is necessary for the specified purpose or purposes;
8. Give a copy of his/her personal data to any individual, on request.

These provisions apply to **ALL** personal data held. Personal data means data relating to a person who is or can be identified either from the data itself or in conjunction with other information that is in, or is likely to come into, the possession of the Department. It covers any information that relates to an identifiable, living individual. This data can be held on computers or in manual files.

The Acts also provide that a "duty of care" is owed to **data subjects**, which means that those

controlling or processing the data should take care that their activities do not cause damage or distress to the people concerned by, for example, maintaining inaccurate information on our files, or disclosing personal data to someone who is not entitled to this data.

The Department holds data to administer its functions. Staff are provided with access to that data in order to do their jobs. **Under no circumstances should data be accessed without a direct business requirement. Confidential customer information must never be discussed with or disclosed to any unauthorised third party, either internal or external.**

4. Application of the Rules of Data Protection

In order to ensure the Department's compliance with the Rules of Data Protection, the following procedures must be observed at all times:

*** Rules 1, 2 and 6 (obtaining and processing all personal data fairly)**

Personal data is obtained fairly if the data subject is aware of the purpose for which the Department is collecting the data at the point of collection and of the categories or person/organisation to whom it may be disclosed. This is a normal part of the claim registration and maintenance function and is noted on Departmental application forms. Investigating Officers also make this clear during the course of any enquiries. **Obtain personal data only when there is a clear purpose for doing so, obtain only that which is necessary for fulfilling that purpose and ensure that it is used only for that purpose.**

Rule 3. (disclosing personal data)

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which it is held. **Do not disclose any personal data to any third party without the consent of the data subject** (see exceptions below). Personal data should not be disclosed to work colleagues unless they have a legitimate interest in the data in order to fulfil official duties.

Permitted disclosures of personal data

Personal data can be disclosed without the express written consent of the data subject in the following circumstances:-

- to the data subject or to a person acting on his/her behalf;
- at the request or with the consent of the data subject or a person acting on his/her behalf;
- where the data subject has already been made aware of the person/organisations to whom the data may be disclosed;
- required by law or a court order;
- required for legal advice or legal proceedings, where the person making the disclosure is a party or witness ;
- required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or a health board;

- authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Síochána not below the rank of chief superintendent or an officer of the Permanent Defence Forces not below the rank of colonel);
- required urgently to prevent injury or damage to health or serious loss of or damage to property;
- required to protect the international relations of the State.

Further detailed guidelines will issue on the procedures to be followed in relation to the disclosure of personal data to authorised third parties.

NOTE: Apart from receiving a query from the data subject or a person acting on his/her behalf, if you receive a request for information required for any of these reasons you should pass it on to your supervisor/manager. If the supervisor/manager has any doubt about the query s/he should contact Business Information Security Unit (BISU).

Rule 4. (securing personal data)

The Department must protect personal data from unauthorised access when in use and in storage and must protect it from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

Personal electronic data should be subject to appropriate stringent controls, such as passwords, access logs, back-ups etc,

Screens, print-outs, documents and files showing personal data should not be visible to unauthorised persons,

Personal manual data should be held securely in locked cabinets, locked rooms, or rooms with limited access,

Special care must be taken where mobile computing and storage devices, such as laptops, are used. **Further Guidelines will issue in respect of mobile devices.**

The Department, as a Data Controller, in disclosing personal data to a Data Processor (e.g. a Branch Office) should only do so under a written agreement, specifying the security arrangements which must be in place.

Rule 5. (accuracy and completeness of personal data)

Data subjects have a responsibility to advise the Department of any errors or changes to data. Once informed, it is imperative that the data be amended accordingly.

Rule 7. (retention and disposal of personal data)

Data should not be kept for any longer than is necessary for the purpose for which it was collected and should not be subject to further processing that is not compatible with that purpose.

Personal data should be disposed of **securely** when no longer required. The method should be appropriate to the sensitivity of the data. Shredding or incineration is appropriate in respect of manual data; and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs or laptops are transferred from one person to another within the Department, or outside the Department, or when being disposed of. **Further detailed guidelines in respect of appropriate retention and disposal procedures are in the Data Retention Policy.**

Rule 8. (rights of data subjects)

The DP Acts provide for the right of access by the data subject to his or her personal information. **Subject Access Requests are dealt with by Data Access Section.** Accordingly, if you receive a request of this nature you should send it to **Data Access Section, Shannon Lodge, Carrick-on-Shannon, for immediate action.**

5. Responsibilities of data subjects

All staff, customers and other data subjects are entitled to be informed how to keep their personal information up-to-date. All staff, customers and other data subjects are responsible for:

checking that any information that they provide to the Department is accurate and up-to-date; informing the Department of any errors or changes to details that they have provided, e.g. change of address;

6. Implementation of Data Protection Guidelines

The Department takes its Data Protection obligations very seriously. All staff and third parties who are authorised to have access to personal data held by the Department must ensure that they are familiar with and adhere to these Guidelines.

7. Breaches of Data Protection.

The Department will investigate all allegations of suspected breaches of data protection. All complaints, from whatever source (e.g. the data subject, staff, management, etc.), should be forwarded to line management who must immediately notify the Head of Information Security (PO, Risk Management Division) who is responsible for the co-ordination of investigations across the Department.

Any breach of trust with regard to the confidentiality of personal data will be treated as serious misconduct under the Disciplinary Code and comes under immediate consideration for dismissal.

8. Further Information

If you have any queries or require clarification on any aspect of these procedures and guidelines, please contact the Business Information Security Unit (BISU), Goldsmith House. All contact with the Data Protection Commissioner's Office should also be channelled

through this section. BISU may be contacted at extension 42744.

Extensive information is available from the Data Protection Commissioner's website www.dataprotection.ie.

Issued 30 July 2008

Updated 25 May 2012

Data Protection Policy

1. Purpose and scope

The Department of Social Protection is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Acts 1988 and 2003. (DP Acts). The Department needs to process (store or use) certain personal data about staff and its customers in order to fulfil its purpose and to meet its legal obligations.

Personal data means data relating to a person who is or can be identified either from the data itself or in conjunction with other information that is in, or is likely to come into, the possession of the Department. It covers any information that relates to an identifiable, living individual. This data can be held on computers or in manual files.

The Department will process such information according to the **Data Protection Principles** that are set out in the DP Acts. It will:-

- * Obtain and process the information fairly;
- * Keep it only for one or more specified and lawful purposes;
- * Process it only in ways compatible with the purposes for which it was given to you initially;
- * Keep it safe and secure;
- * Keep it accurate and up-to-date;
- * Ensure that it is adequate, relevant and not excessive;
- * Retain it no longer than is necessary for the specified purpose or purposes;
- * Give a copy of his/her personal data to any individual, on request.

The Acts also provide that a "duty of care" is owed to data subjects, which means that those controlling or processing the data should take care that their activities do not cause damage or distress to the people concerned by, for example, maintaining inaccurate information on our files, or disclosing personal data to someone who is not entitled to this data.

To ensure that all staff and others who process personal data on behalf of the Department are doing so in accordance with these principles at all times, the Department has developed this Data Protection Policy together with a series of detailed guidelines, the Data Protection Policy Guidelines.

2. Role of the DSP

The Department is the **data controller** under the DP Acts and is ultimately responsible for the implementation of the DP Acts in respect of the data for which it has responsibility.

The Department has appointed a Head of Information Security, who is the Department's

primary contact to the Data Protection Commissioner and is responsible for the co-ordination of DP issues across the Department, ensuring the provision of suitable DP advisory, training and awareness services and advising senior management on relevant DP issues.

The Department will annually notify the Data Protection Commissioner that personal data is being processed and list the categories of personal data that are being processed.

3. Governance

This policy has been approved by the Secretary of the Department and is one of several information security policies which support the Department's corporate plan and information strategy. It will be reviewed regularly.

Principal Officers are responsible for ensuring that this policy is implemented in their respective Divisions. Managers at all levels are responsible for ensuring that their staff observes its provisions.

If anyone considers that this policy has not been followed, they should raise the matter through their line management with the Head of Information Security.

4. Rights of data subjects (i.e. customers, staff and third parties) to access to personal data

Data subjects include staff and customers of the Department and any other person about whom the Department processes data.

All data subjects have the right to access the information held about them, ensure that it is correct and fairly held, and to complain to the Data Protection Commissioner if they are dissatisfied.

All requests to access personal data will be handled in accordance with the procedures as detailed in the Data Protection Policy Guidelines.

5. Responsibilities of staff and third parties

5.1 Persons who process personal data on behalf of the Department

Anyone who processes personal data on behalf of the Department has a responsibility to ensure that the **Data Protection Principles** are observed.

Detailed advice on how to achieve this is given in the Data Protection Policy Guidelines.

5.1.1 Staff

Staff who, as part of their responsibilities, process personal information about other people, must comply with this policy and the associated Guidelines.

5.1.2 Others working for or on behalf of the Department

Others working for/on behalf of the Department, usually called third parties, who handle personal data in connection with the Department, must operate in accordance with the DP Acts and details of such processing should be the subject of written agreements between the Department and the third party. See the Data Protection Policy Guidelines for further details.

5.2 Persons who provide personal data to the Department

Everyone who provides personal data to the Department is responsible for ensuring adherence to the Data Protection Principles, especially with regard to accuracy and, in the case of third parties providing the personal data of others, the right to disclose this personal data.

Policy was issued 30 July 2008

Policy updated 11 May 2012

Guidance Note for Staff

Disclosure of Personal Data

1. Introduction

This Guidance Note is intended as a further aid to staff in the implementation of aspects of the Department's Data Protection Policy and Guidelines and should be read in conjunction with them. Copies of these are available on the Business Information Security Unit (BISU) Webpage. Its purpose is to assist frontline staff in dealing with requests for personal information.

It should be remembered that the Department holds personal data to perform its administrative functions. Staff are provided with access to that data in order to do their jobs.

These are only guidelines - where you have any doubt about a particular request or indeed the 'bona fides' of the person making the request, you should seek the advice of your Supervisor/Manager or Business Information Security Unit (BISU) before disclosing any personal data.

Note:- Under no circumstances should personal data be accessed without a direct business requirement and it must never be discussed with nor disclosed to any unauthorised third party. Failure to adhere to this requirement could have serious repercussions for the staff member concerned, including possible sanction under the CS Disciplinary Code (up to and including possible dismissal) and possible legal action.

2. What does this mean for me? Some practical DO's and DON'Ts:

Insofar as the provisions of the Data Protection Acts relating to the disclosure of personal data affect the routine work of staff in this Department, its principal requirements can be translated into a few practical DO's and DON'Ts:

DO

- Record information accurately and keep it up to date.
- Keep your work area clear of confidential data when not in use.
- Observe computer security procedures.
- Firmly establish the identity of an enquirer before disclosing any personal information and make sure that the enquirer has a right to this information.
- Only give as much information to answer the question asked.
- Ask your supervisor if you are in any doubt about giving out any information.
- Keep a record of the disclosure on the relevant file.

DON'T

- Give out any personal data unless you know the identity of the enquirer and you are satisfied that the person is entitled to the information.
- Give details of a customer's Personal Public Service Number (PPSN), name, address, date-of-birth, birth surname or mother's birth surname, to **ANYBODY** other than the customer themselves.*
- Disclose your password to a colleague.
- Leave your terminal logged on when you leave your desk.
- Let your VDU/PC or computer printout be seen by unauthorised individuals.

*** There are some exceptions to this, notably where data sharing is governed by legislation. Please see Appendices 2 and 3 for information on who is entitled to have access to / use the use of the PPSN.**

2.1 Good Practices

One way of ensuring that information is not disclosed to the wrong people is to develop good practices when dealing with it. The following are some examples of good practice:-

- ✓ If you work in an office to which the public has access, make sure that any data on your VDU/PC screen, your papers and your computer printouts are not legible to the public unless you want them to see relevant details e.g. if discussing entries on a form. Putting paper and printouts away after each enquiry is good practice.
- ✓ When you leave the VDU/PC for a period, be sure to lock the computer, or log-off the network. This is important not only for data protection/security but also for preventing fraud.
- ✓ At the end of the day, log-off the VDU/PC and file away any papers or documents containing sensitive data that you are finished with.
- ✓ In as far as is practical, adopt a 'clear desk' policy – i.e. keep your workspace clear of **confidential** data.
- ✓ **NEVER** disclose your password.

3. Authorised Disclosure of Personal Data

3.1 Data Protection Act

Section 8 (b) of the Data Protection Acts states that any restrictions in the Acts on the processing of personal data do not apply *“if the processing is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would*

be likely to prejudice any of the matters aforesaid.”

Personal data **can** be disclosed without the express written consent of the data subject in the following circumstances:-

- ✓ to the data subject or to a person acting on his/her behalf;
- ✓ at the request or with the consent of the data subject or a person acting on his/her behalf;
- ✓ where the data subject has already been made aware of the person/organisations to whom the data may be disclosed;
- ✓ required by law or a court order;
- ✓ required for legal advice or legal proceedings, where the person making the disclosure is a party or witness;
- ✓ required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or the HSE;
- ✓ authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Síochána not below the rank of chief superintendent or an officer of the Permanent Defence Forces not below the rank of colonel);
- ✓ required urgently to prevent injury or damage to health or serious loss of or damage to property;
- ✓ required to protect the international relations of the State.

Note: Apart from receiving a query from the data subject (or a person acting on his/her behalf) or as provided for below, if you receive a request for information required for any of these reasons you should pass it on to your supervisor/manager. If the supervisor/manager has any doubt about the query, s/he should contact Business Information Security Unit (BISU).

3.1.1 Enquiries from An Garda Síochána

Data Protection legislation permits the disclosure of information to members of An Garda Síochána **when they are investigating offences**. A letter/fax signed by a Garda Sergeant on the Garda Station's headed notepaper confirming that the information is required in relation to the investigation of an offence should be requested before any information is divulged. **Only Information relevant to the investigation should be disclosed.**

In addition, Section 8 of the Immigration Act 2003 permits the exchange of information with An Garda Síochána in respect of non-nationals. The procedures outlined above should be followed in these cases also.

See Frequently Asked Questions in Appendix 1 for more detailed information on how to handle Garda requests.

3.2 Social Welfare Legislation

3.2.1 Exchange of information for the control of schemes

Section 261 of the SW Consolidation Act 2005 provides for the exchange of information to/from a range of public bodies for the purposes of the Act and the control of schemes. This Section may be relied upon by Control Sections across the Department under authorisation from the Principal Officer with responsibility for the data concerned.

3.2.2 Sharing of information with specified bodies

Sections 265 to 270 of the SW Consolidation Act 2005 provides for the disclosure of personal information to a number of public bodies in certain circumstances, without the necessity to obtain the customer's explicit consent. A list of these organisations is attached – see Appendix 3 or, alternatively, visit the BISU Website.

Information may be shared with a specified body that has a **transaction with the customer** relating to a benefit, Health, Education or Local Authority payment/service or free civil legal aid. The specified body can only seek information in relation to a transaction relating to one of these purposes.

If a request relates to an individual, the information may be disclosed provided you are satisfied that the request has come from one of these organisations, that the organisation has a transaction with the person concerned and that the information being sought is relevant (and not excessive) to the specified purpose.

If the request is for information about groups of customers, the organisation should send the request **in writing** to the Principal Officer of the area in the Department holding the information, specifying the relevant legislation under which they are seeking the information. If the release of information is authorised, it should be remembered that it is the Department's policy that **all bulk transfers of personal data must take place over secure direct links and/or be encrypted**, in accordance with the Department's **External Party Electronic Data Transfer Policy**.

Business Information Security Unit must be advised of **all** such requests as a matter of course. Managers should ensure that procedures are in place to notify BISU of all bulk transfers. BISU will maintain a register of all bulk data transfers.

In general, requests from organisations for personal data should be dealt with in writing. Routine enquiries from the HSE and the Revenue Commissioners, however, may be dealt with over the telephone, once the identity of the caller has been established.

A growing number of public bodies have adopted the PPSN as a unique customer identifier because it facilitates speedy and accurate identification of individuals accessing public services. This has led to an increase in the number of enquiries requesting PPS Numbers. All of the Specified Bodies listed in Appendix 3 are entitled to request a person's PPSN. Staff should note that a Specified Body's right to request a PPSN is predicated on it being able to establish the need as relevant and necessary in accordance with a customer's transaction with it. **See Appendix 2 for detailed advice on handling requests for PPS Numbers.**

3.3 Enquiries from other Social Security Authorities

EU Regulations allow for the exchange of relevant customer information (e.g. claim data, social insurance record etc.) with Social Security authorities in other EU countries.

Example:- Control Sections may receive telephone enquiries from the UK Department of Work and Pensions and in such cases data may be disclosed, provided the information is required for the purpose of detecting and investigating fraud or other criminal offences.

In addition, the Department has Bilateral Agreements with Social Security agencies in Australia, Canada, New Zealand, Quebec, the Swiss Confederation, South Korea and the US, which allow for similar exchange of customer information with these agencies.

This exchange of customer information is usually done through designated sections (e.g. Control Division, EU Payments, EU Records etc.) in the Department.

4 Procedures for Dealing with Requests for Personal Data

In the normal day-to-day running of the section you may receive enquiries from various sources, including:

- Telephone Enquiries
- Enquiries in the Public Office
- Written Enquiries
- E-Mail Enquiry

4.1 Telephone Enquiries

If you receive a telephone enquiry, there are some standard steps you should take:

➤ **Establish the identity of the caller.**

- If the person making the call claims to be the subject of the data request, ask for identifying details such as Personal Public Service Number (PPSN), date of birth, mother's birth surname (maiden name) and any other personal information which may help to verify that the person making the enquiry is who s/he says s/he is.
- If the caller claims to be acting on behalf of a customer (e.g. a relative, legal representative, Citizen's Information Services etc.), you must not only satisfy yourself as to the caller's identity, but also **confirm that s/he has the authority to act on the customer's behalf**. At least the name, address and telephone number of the enquirer should be obtained. Also establish the enquirer's relationship with the customer and the reason why s/he is acting on the customer's behalf. This will frequently be apparent by virtue of the nature of the enquiry. **If you have any doubt as to the bona fides of the enquirer, no information should be disclosed.** Keep a record of the call.
- If the caller is a public representative, information on a case may be disclosed once you have established that the caller is a public representative and is acting on behalf of the data subject. However, it should be noted that the

disclosure of a customer's PPSN is not permitted (See Appendix 2).

- **Only give information which is needed to answer the question.**
- If dealing with an enquiry that would involve disclosing information of a particularly personal nature, seek clearance from your Supervisor/ Manager or arrange to post the information to the data subject.
- Always **keep a record of the disclosure** on the relevant file.

4.2 Enquiries in the Public Office

The same precautions as outlined at 3.1 above should be exercised in dealing with enquiries made in person in a public office. In addition, however, you should try to obtain some means of identification from the enquirer (e.g. passport, driving licence or utility bill).

4.3 Written Enquiries

You should have no difficulty replying to written enquiries from a customer in relation to aspects of his/her personal data as the information will be going directly to the data subject. The envelope should be marked "Private and Confidential". In the case of sensitive personal information, e.g. containing health details, correspondence should be by registered post.

If a written enquiry is received from a third party, the customer's authorisation to give the information requested should be obtained and authenticated, e.g. by comparing the customer's signature on a letter of consent against that held on file.

In the case of written enquiries from a public representative, solicitor or accountant acting on behalf of the customer, the customer's authorisation can be assumed.

If you are in any doubt about a case, you should discuss it with your Supervisor / Manager, or BISU, as appropriate.

4.4 E-Mail Enquiries

Due to the risk of 'phishing', you must be extremely careful in relation to handling email requests for personal details. Phishing is the criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy source in electronic communication. **Personal details should not be sent by e-mail to individual customers.** The person should be advised that a written reply will be posted to the home address of the customer. Only general information should be sent by e-mail.

Subject to the provisions of Section 3 above, personal information can be sent by e-mail to certain public bodies. If you are in any doubt about the e-mail address of the enquirer, contact IS Services Helpdesk at Ext 44111.

4.5 FAX Enquiries

In the case of FAX enquiries, it is often very difficult to establish and authenticate the source of the enquiry. Where the identity of the caller cannot be authenticated by other means (e.g. phone verification), personal information should not be disclosed in FAX responses. In such

cases, the enquirer should be informed that the information requested will be posted to the home address of the customer.

5. Instructions to Staff when logging-on to DSP Computer Systems

‘Log-on’ Messages are displayed when entering the Department's computer systems, reminding staff that personal data must be safeguarded, regarded as confidential at all times and must **never** be accessed except for a valid business purpose.

6. Abuse/Misuse of Personal Information held by the Department

The Department takes its obligations as a data controller very seriously and adopts the strongest line in relation to the abuse/misuse of customer information by any of its staff. Any breach of trust with regard to the confidentiality of information is treated as serious misconduct under the Disciplinary Code and comes under immediate consideration for dismissal. In addition, a breach of the Data Protection Acts is a criminal offence and could lead to prosecution.

7. Data Access Requests

The Data Protection Acts gives ALL our customer's the right:-

- ✓ to determine whether the Department holds any personal information relating to them;
- ✓ to be supplied with a copy of this data, if they so request;
- ✓ to have this data amended or erased if it is incorrect;
- ✓ to seek the assistance of the Data Protection Commissioner.

If a customer wishes to obtain a copy of their personal information then the request must be made in writing and should clearly specify that the request is a Data (or Subject) Access Request. Such requests must be accompanied by the appropriate fee (currently €6.35).

THESE REQUESTS SHOULD BE FORWARDED IMMEDIATELY TO DATA ACCESS SECTION, SHANNON LODGE, CARRICK-ON-SHANNON, CO. LEITRIM.

Footnote:- The DSP Data Protection Policy and Guidelines are updated on an ongoing basis by BISU to take account of legislative change.

APPENDIX 1

FREQUENTLY ASKED QUESTIONS IN RELATION TO GARDA REQUESTS

Q:- Should verification that the information is being requested in connection with the investigation of a crime (or Section 8 of the Immigration Act 2003) be sought?

A:- Yes. A letter or a fax signed by a Garda Sergeant on the Garda Station's headed paper must be supplied (before information is disclosed) confirming that the information is being sought in connection with the investigation of a crime or Section 8 of the Immigration Act 2003.

Q:- Can the information be given by phone?

A:- No. Under no circumstances should confidential customer information be disclosed over the phone.

Q:- Can any information requested be given?

A:- No- only information certified as being relevant to an investigation or required under Section 8 of the Immigration act 2003 can be disclosed. Note, however, that An Garda Siochana do have the authority to request details of the family / relatives of an individual provided this information is certified as being relevant. It would be unusual for a PPS Number to be relevant to the investigation of a crime.

Q:- Should a record be kept of the information given and to whom it was given?

A:- Yes. A copy of the request (see above) and reply should be retained on the customer's file for record purposes.

Q:- Should there be nominated persons at both sides as a control measure in the exchange of information?

A:- No. This would be impractical as the nominated persons would not always be available.

Q:- If the request for information is stated to be in connection with a missing person, should any information requested be given, bearing in mind that the "missing" person may not want to be found?

A:- An Garda Siochana do have the authority to request information on a missing person.

Q:- What if a Garda comes into a DSP office in person requesting information?

A:- The Garda should be asked to provide ID. S/he should also supply a letter or a fax signed by a Garda Sergeant on the Garda Station's headed paper, confirming that the information is being requested in connection with the investigation of a crime or Section 8 of the Immigration Act 2003. A record should be kept of the information given.

APPENDIX 2

FREQUENTLY ASKED QUESTIONS IN RELATION TO REQUESTS FOR PPSNs

➤ **A customer is looking for his/her PPS Number**

If a customer is looking for his/her own PPS Number, s/he should be asked to supply the following information:-

- ✓ Name
- ✓ Date of Birth
- ✓ Address
- ✓ Mother's Birth Surname

If the address on our records does not match the address supplied, ask the person for previous addresses. Do not call out the address and ask the person if they ever lived there. Where suspicions are aroused, an officer should delve deeper, asking questions relating to employment or claim history, for example. Only when you are satisfied regarding the caller's identity, should the PPS Number be disclosed.

➤ **A customer is looking for his/her child's PPS Number**

If a customer is looking for his/her child's PPS Number, first ask for the child's age as the PPSN can only be disclosed if the child is under 16 years of age. S/he should then be asked to supply the following information:

- ✓ His/her own name
- ✓ His/her own PPS Number
- ✓ His/her own Address
- ✓ Child's Date of Birth
- ✓ Child's Mother's Birth Surname.

If the child's PPS Number is traced, check if s/he is linked to the parent on CRS. This can be checked by using the RDRelationship Detail option on Infosys. If the child is not linked to the parent on CRS, the Number cannot be disclosed. When you are satisfied with the caller's identity and that s/he is the parent of the child, the child's PPS Number may be disclosed.

In the case of a child over 16 years, the PPSN should not be disclosed over the phone, but may be sent by post to the listed home address of the child.

➤ **A customer is looking for his/her spouse's or partner's PPS Number**

A customer should not be given their spouse or partner's PPS Number. S/he should be advised to ask the spouse or partner to contact the Department directly.

➤ **A Solicitor or Accountant is looking for a customer's PPS Number**

Requests of this nature should be writing. If you are satisfied that the Solicitor or Accountant is acting on behalf of the customer, the PPS Number can be disclosed.

➤ **A Public Representative is looking for a customer's PPS Number**

The Public Representative should be advised that we are not permitted (S.262(9) of the Social Welfare Consolidation Act, 2005 refers) to disclose this information without the written consent of the customer. You may however, write directly to the customer with the information.

➤ **A Government Department or Public Body is looking for a customer's PPS Number**

Check that the Third Party are legally entitled to use the PPS Number. The list of Specified Bodies authorised to use the Number is in Appendix 3 of these Guidelines. It is the duty of all bodies to ensure that they are specified in law as being so entitled, before they request or hold a record of any person's PPS Number.

APPENDIX 3

Authorised Bodies

The SW Consolidation Act 2005 (Sections 265 – 270) provides for the disclosure of personal information **in certain circumstances** (see Section 3.2.2 above) with the following Bodies:-

- a Minister of the Government,
- Commission for Public Service Appointments,
- Public Appointments Service,
- Revenue Commissioners;
- a local authority (for the purposes of the Local Government Act, 2001),
- a vocational education committee (within the meaning of section 7 of the Vocational Education Act 1930)
- the Health Service Executive,
- a body established by the Minister for Education and Science under section 54 of the Education Act 1998,
- An Foras Áiseanna Saothair,
- An Garda Síochána and the Defence Forces in respect of their own members,
- An tArd-Chláraitheoir,
- an tUdaras um Ard-Oideachas,
- Coillte Teoranta,
- Enterprise Ireland,
- National Education Welfare Board,
- Central Applications Office,
- Central Statistics Office,
- Commission for Taxi Regulation;
- Companies Registration Office,
- General Medical Services (Payments) Board,
- Legal Aid Board,
- Mental Health Commission,
- National Breast Screening Board,
- National Cancer Registry Board,
- National Council for Special Education,
- The Pensions Board,
- The Pensions Ombudsman
- Personal Injuries Assessment Board,
- Private Residential Tenancies Board,
- Private Security Authority,
- The Health & Social Care Professionals Council
- The Probate Office

- The Property Services Regulatory Authority
- The Road Safety Authority
- Sustainable Energy Ireland – The Sustainable Energy Authority of Ireland
- The Teaching Council.

The following Voluntary Hospitals:-

- Beaumont Hospital, Dublin,
- Cappagh National Orthopaedic Hospital, Dublin,
- Coombe Women's Hospital, Dublin,
- Dublin Dental Hospital,
- Hume Street Hospital, Dublin,
- Incorporated Orthopaedic Hospital of Ireland, Clontarf, Dublin,
- Leopardstown Park Hospital,
- Mater Misericordiae University Hospital, Dublin,
- Mercy Hospital, Cork,
- National Maternity Hospital, Dublin,
- National Rehabilitation Hospital, Dun Laoghaire,
- Our Lady's Hospice, Dublin
- Our Lady's Hospital for Sick Children, Crumlin, Dublin,
- Portiuncula Hospital, Ballinasloe, Co. Galway,
- Rotunda Hospital, Dublin,
- Royal Victoria Eye and Ear Hospital, Dublin,
- South Infirmary/Victoria Hospital, Cork,
- St. James's Hospital, Dublin,
- St. John's Hospital, Limerick,
- St. Luke's Hospital, Dublin,
- St. Mary's Hospital and Residential School, Baldoyle, Dublin,
- St. Michael's Hospital, Dun Laoghaire,
- St. Vincent's University Hospital, Elm Park, Dublin,
- St. Vincent's Hospital, Fairview,
- The Adelaide and Meath Hospital, Dublin incorporating the National Children's Hospital,
- The Children's Hospital, Temple Street, Dublin,
- The Royal Hospital, Donnybrook,

University Dental School and Hospital, Cork

Note:- List of Authorised Bodies updated 3 April 2013.