DEPARTMENT OF AGRICULTURE, ENVIRONMENT AND RURAL AFFAIRS

DATA PROTECTION POLICY STATEMENT

Department of
Agriculture, Environment
and Rural Affairs

January 2017

Table of Contents

DATA PROTECTION POLICY STATEMENT

Introduction

1. The Department of Agriculture Environment and Rural Affairs holds and processes a large quantity of personal information which has been generated by our business over the years. Such information is held in a variety of formats, including computer records, structured and unstructured manual records, mobile devices, photographs, microfiches and CCTV surveillance on digital media. It relates to both staff and members of the public and includes factual information (such as names, addresses and contact numbers) and opinions (such as staff reports).

2. The Freedom of Information Act 2000 determines the disclosure of the majority of information held by the Department, including personal information relating to third parties. The Data Protection Act 1998 controls how personal information must be treated. Personal Information is defined as "Data which relates to an individual who can be identified – (a) from that information or (b) from those data or other information which is in the possession of, or is likely to come into the possession of, the data controller." The Data Protection Act 1998 is intended to protect personal privacy and to support the rights of individuals by regulating the processing of their personal information. It gives specific rights to individuals about whom personal information is held and places specific responsibilities upon those holding or processing that personal information.

3. Individuals are entitled to use the Data Protection Act 1998 to ask for all personal information that the Department holds about them and whether it is held within a structured filing system or not.

4. Every year the department deals with a number of information access and data protection requests involving personal information. The Information

Commissioner (ICO), who operates as an independent public official reporting directly to Parliament, has responsibility for ensuring that public authorities comply with the requirements of all information access legislation. The ICO has authority to take enforcement action against those which do not comply. This action now includes the enhanced power to impose a monetary penalty of up to £500,000 for any breaches under the Data Protection Act. It is important, therefore, that all staff in the Department who hold or process personal information are familiar with the legislative requirements and the implications of this Data Protection Policy Statement.

Objectives

5. The objective of the Data Protection Policy Statement is to show the Department's commitment to comply with the Data Protection Act 1998, in relation to the following:
   - Quality: all personal data held by the Department must be accurate and kept up to date;
   - Use: all personal data held by the Department must be used only for the purpose or purposes for which it was collected;
   - Awareness: all staff whose work involves personal data must be fully aware of legal requirements relating to the holding and processing of this data;
   - Accountability: staff who deal with personal data should be personally responsible for their actions;
   - Confidence: everyone whose personal data is held by the Department needs to be assured that their lives will not be adversely affected as a result of incorrect processing of their data.

While it is intended that this Policy Statement will prove useful in setting out the ground rules for those dealing with personal information, staff are encouraged to find out more about the details of the legislative requirements that have to be met by consulting the Information Management Branch intranet site.

Policy Statement

6. The Department regards the fair and lawful treatment of personal information as a critical factor in the success of our operations and a key to the maintenance of the confidence that exists between those with whom we deal and ourselves. The Department therefore acknowledges its legal obligations under the Data Protection Act and endorses its requirements.

7. In order to carry out our duties, members of staff in many business areas need to collect and use specific information about individual people or groups of people. These include members of the public, people who work for the Department or have done so in the past, suppliers, contractors, farmers and many others. Such information must be managed properly regardless of how or why it is collected and irrespective of how it is currently held. The Department will take steps to ensure compliance with current and possible future legislation in the area of Data Protection.

8. In the case of personal information relating to current members of staff, HR Connect now requires members of staff to input their own personal data. Each member of staff is responsible for the accuracy of his/her own personal data and for compliance with the Department's obligations in this regard.

9. The Data Protection Act is centred on 8 Data Protection Principles.

    1) personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
    2) personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner which is incompatible with those purposes (in order for personal data to be used by the collector for a different purpose, or shared with another part of

the Department, it should be made clear at the time of collection that the data being collected may be used in such ways);

3) personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is obtained;
4) personal data shall be accurate and, where necessary, kept up to date;
5) personal data processed for any purpose shall not be kept for longer than is necessary for that purpose;
6) personal data shall be processed in accordance with the rights of the data subject;
7) appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against loss, damage or destruction of that data;
8) personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures a similar level of protection for the rights and freedoms of data subjects in relation to the processing of personal data exists in that country or territory.

The Department tries, through appropriate management and strict controls to comply with these principles:

10. The Data Protection Act also gives a number of rights to those about whom we hold personal information (data subjects). The Department acknowledges these rights and is committed to protecting them in the way in which it holds and processes personal data. The specific rights given to data subjects are as follows:

- the right to know if the Department is processing personal data relating to them as individuals and the right to request a copy of that data and any associated information. This associated information could be the source of the data or the interpretation of any codes or symbols used to describe the data. A request for this type of information is called a Subject Access Request (SAR) and it must be dealt with within the 40 calendar day legislative deadline. As mentioned in paragraph 1, opinions are covered by the Data Protection Act. This information is also disclosable under a SAR. In view of this, it is recommended that

subjective or personal opinions about a named individual are recorded **only with good reason**;

- the right to prevent processing of personal data if it is likely to cause the data subject unwarranted substantial damage or distress;
- the right to object to automated processing if it is likely to result in a decision that substantially affects the data subject;
- the right to compensation, payable by the Department, for damage and distress caused to the data subject by any contravention of the Act;
- the right to require the Department, in certain circumstances, to rectify, block, erase or destroy personal data;
- the right to ask the Information Commissioner to assess whether or not it is likely that any processing of personal data has been or is being carried out in contravention of the Act.

11. In order to uphold the rights of data subjects the Department will ensure that:
    - there is a Data Protection Officer appointed with specific responsibility for data protection (this is currently Mark Maxwell, Information Management Branch, ext 24238);
    - everyone processing personal information is appropriately trained and supervised, and that they understand that they are directly and personally responsible for following good data protection practice;
    - queries about processing personal information are dealt with promptly and courteously;
    - methods of processing personal information are described clearly and evaluated regularly;
    - actual performance in the processing of personal information is assessed regularly.

12. The Department's Privacy Notice (Appendix 1) provides a useful summary of how the Department is entitled to use or process the personal information it holds. The wording of this notice has been approved by the Information Commissioner's Office. It should be incorporated into all

forms used by the Department for the collection of personal information so that data subjects know how the Department intends to process their personal details. This enables business areas to share personal data between each other so long as it is for "legitimate purposes" in line with the Data Protection Act 1998 and Freedom of Information legislation. Personal information which is not collected under the Fair Processing Notice may normally be used only for the purpose(s) for which it is collected. This places automatic limitations on how it can be shared across the Department. Data subjects are entitled to be informed at the time personal information is collected how it will be used and any wider use is in contravention of the Data Protection Act. It is particularly important to note this at a time when developments in mobile computing and information technology have made the potential for the easy transfer of information so much greater than it was in the past. Any business area considering sharing personal information with another business area should consult IMB first before taking any other action. Because information can only be used for the purpose for which it was gathered the sharing of information between business areas may require a Data Sharing Agreement to be put in place. Details of this agreement can be obtained from IMB.

13. The sharing of bulk personal information to enable another public body to trawl through it for its own purposes is not allowed under the Data Protection Act. This does not mean that the Department will not provide personal information to other organisations. Sometimes the department is required to provide this information in order to facilitate, for example, fraud or criminal investigations. Under these circumstances the Department will provide specific information about an individual or number of individuals who are under investigation. This is distinct from bulk personal information about a particular class of data subjects (e.g. farmers or employees). This information will not be provided except in special circumstances where the organisation has specific statutory powers to request such information. Any business area receiving requests for personal information of this type should consult IMB before taking any other action.

14. Some of the personal data which the Department holds falls into the category of sensitive personal data. Types of data regarded as sensitive include information about a person's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions. The requirements for processing sensitive personal data are more strict than those for other personal information. The normal requirements for the processing of personal data are outlined in Schedule Two of the Data Protection Act 1998 and the additional requirements relating to sensitive personal information are detailed in Schedule 3. A summary of the list of the requirements of both Schedules is attached at Appendix 2. The Department will ensure that any sensitive personal data it holds is processed in accordance with these requirements.

15. The department often receives Freedom of Information requests involving the personal information of members of staff or others. Whenever this happens the Department is committed to ensuring that the 8 Data Protection Principles outlined in paragraph 8 are applied fairly. All legislative requirements intended to safeguard personal information must be met.

16. It is extremely important that the Department is able to demonstrate that it takes adequate steps to safeguard the personal data and sensitive personal data it processes. This applies equally when it is being processed by others on the Department's behalf (as with HR-Connect for example). Under these circumstances the processing organisation must provide guarantees about the security of the processing being done for the Department. These guarantees must be in the form of a written contract. Security measures must be at least equivalent to those we would apply if doing the job ourselves. If any security breach involving personal data occurs this must be reported to the relevant authority in line with AEC 12/10 and also in accordance with their own business area's Information Loss Reporting and Handling Plan.

17. As a holder of personal information the Department is legally obliged to notify the Information Commissioner and to provide a description of the types of personal information processed. This information is entered in the Data Protection Register, which lists all data controllers, and is made available to the public on the Information Commissioner's Website. Notification is renewable annually and the Department is committed to keeping its entry current at all times. The annual renewal exercise is coordinated by Information Management Branch (IMB) but business areas must inform IMB as and when an amendment is required throughout the year. It is a legal requirement that all changes to the Department's notification are made known to the Information Commissioner's Office within 25 days of the change occurring.

Implementation

18. Responsibility for delivering the actions outlined in paragraph 10 rests with both Information Management Branch and business areas. IMB plays a central role in terms of raising awareness, providing advice any complaints. However, it is the responsibility of heads of business areas to review procedures, to monitor performance and to satisfy themselves that all members of staff who deal with personal information are fully aware of their responsibilities and follow correct procedures to ensure they comply with the Data Protection Act 1998. Heads of business areas, at all levels, are responsible and accountable for the information held and processed by their business area.

19. Specific actions to be taken by IMB include:
    - making available to business areas the information they require to comply with the legislation. This will include publicising this policy, putting information on the intranet, ensuring adequate training is available, liaising with business areas, responding to queries from business areas and inputting to induction procedures;

- confirming with business areas on an annual basis that they are content with the data processing procedures they have in place;
- coordination of the annual review of the Department's entry in the Data Protection Register;
- investigation of complaints.

20. Specific actions to be taken by business areas include:

- ensuring relevant staff are trained and are familiar with the requirements of the Data Protection Act and that necessary procedures are in place and followed by staff;
- ensuring all personal information is accessible in the event that it is requested by a data subject;
- ensuring requests for personal information are dealt with within the legislative deadline;
- ensuring that personal information is kept secure, is accessible only to those who need to process it for approved purposes, and is only transferred to other organisations or disposed of appropriately in accordance with the Department's procedures and the requirements of the Data Protection Act. Advice on when it is appropriate to use techniques like encryption should be sought from Information Systems Branch;
- reporting any breach of personal data security to the relevant authority in line with AEC 12/10 and in accordance with their own business area's Information Loss and Reporting Handling Plan at once;
- ensure that all laptops are encrypted and that staff who need to use portable media devices follow the procedures as laid down in the DAERA Removable Media Storage Guidelines.
- ensuring that data protection procedures are documented (for example, in office procedures manuals and job descriptions);
- reviewing internal procedures annually;
- updating the Department's entry in the Data Protection Register within 25 days of any change (this is done through IMB);

- liaising with IMB about any data protection issue they are unsure about.

The Main Decision Maker within each business area has specific responsibility for ensuring these aspects are taken forward.

Conclusion

21. Under this Data Protection Policy, overall responsibility for complying with the requirements of the Data Protection Act 1998 rests with the Permanent Secretary. In practice, however, many of the functions are devolved to the Data Protection Officer who is expected to oversee compliance in conjunction with Heads of Branches. The Data Protection Officer and other staff in Information Management Branch are available to advise on issues which arise. All staff in business units, including Agencies, who process personal information should ensure that their job descriptions and, if necessary, their Personal Development Plans and Personal Performance Agreements, include these responsibilities.

22. The Department will review its procedures regularly to ensure continued compliance with this Policy Statement which, itself, will be reviewed by Information Management Branch at 3 yearly intervals.

Glossary of Terms

Data controller – a person or organisation, like DARD, holding/using personal data and determining how and why information is processed. As a data controller an employer has a responsibility to establish workplace practices and policies that comply with the Data Protection Act 1998.

Data subject – an individual to whom personal information relates; within the workplace a data subject may be a current or former employee or someone applying for a job but a data subject could also be a customer, client, supplier or indeed anyone about whom personal information is held.

Privacy Notice – a statement of how the Department may process personal information. The Privacy Notice is to be included on all forms used for the collection of personal information.

Information Commissioner – this is an independent public official reporting directly to Parliament.

Notification – the Data Protection Act 1998 requires each data controller to notify the Information Commissioner about its personal data processing activities.

Personal data/Personal information – personal information about an identifiable living individual; it can be factual or an opinion.

Processing – this is any activity that involves personal data, including collecting, recording, retrieving, consulting, holding, disclosing or using it; also doing work on the data such as organising, adapting, changing, erasing or destroying it. The Data Protection Act 1998 requires that personal data be processed fairly and lawfully so data controllers have to meet certain conditions. A data subject must be told the identity of the data controller and why his or her personal information is being or will be processed.

Processing personal data – this can be done only where at least one of the conditions set out in Schedule 2 of the Act has been met (see Appendix 2).

Processing sensitive personal data – this can be done only where at least one of the conditions set out in Schedule 2 of the Act and at least one of the conditions set out in Schedule 3 of the Act have been met (see Appendix 2).

Sensitive Personal Data – sensitive personal data includes information about an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions.

Appendix 1

Privacy Notice

The Department takes data protection and freedom of information issues seriously. It takes care to ensure that any personal information supplied to it is dealt with in a way which complies with the requirements of the Data Protection Act 1998. This means that any personal information you supply will be processed principally for the purpose for which it has been provided. However, the Department may also use it for other legitimate purposes in line with the Data Protection Act 1998 and Freedom of Information legislation. These include:

- Administration of the Common Agricultural Policy and other aid schemes;
- The production and safety of food;
- Management of land and other environmental controls;
- Animal health and welfare;
- Compilation of statistics;
- Disclosure to other organisations when required to do so; and
- Disclosure under the Freedom of Information Act 2000 or the Environmental Information Regulations 2005 where such disclosure is in the public interest.

[This is an indicative summary – for more detail please refer directly to the Data Protection Act 1998]

Processing of personal data can only be carried out where at least one of the following conditions set out in Schedule 2 of the Data Protection Act 1998 has been met. Processing must be:

- with the consent of the data subject
- necessary for the performance of a contract with the data subject
- for the compliance with any legal obligation (other than contractual)
- to protect the vital interests of the data subject
- to carry out public functions
- to pursue legitimate interests of the data controller unless prejudicial to the legitimate interests of the data subject.

To process sensitive personal data at least one of the conditions set out in Schedule 2 of the Data Protection Act 1998 must be met **and, in addition**, at least one of the following conditions set out in Schedule 3 of the Act must also be met. Processing must be:

- with the explicit consent of the data subject
- necessary to comply with the data controller's legal duty in connection with employment
- to protect the vital interests of the data subject or another person
- carried out by certain non-profit bodies
- where the information has been made public by the data subject
- in legal proceedings, to obtain legal advice, or exercise legal rights
- to carry out public functions
- for medical purposes
- for equality opportunities monitoring
- as specified by Order made by the Secretary of State