

Department of Agriculture, Environment and Rural Affairs (DAERA)

Data Protection Policy Statement

29 August 2018



**Document information**

Document details

|  |  |
| --- | --- |
| Document name: | Data Protection Policy Statement |
| Document version: | 0.1 |
| Document date: | 29 August 2018 |
| Document status: | Final |
| Authors: | Sinéad Harkin, Departmental Data Protection Adviser |
| Owner: | Philip Gilmore, Departmental Data Protection Officer |
| HPRM (TRIM) reference: | AE1/18/736547  |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Reason for change | Date | Comments |
| 0.1 | Initial draft  | 05/06/18 |  |
| 0.2 | DIM Revision | 18/06/18 |  |
| 0.3 | DPO Revision | 09/08/18 |  |
|  |  |  |  |

Distribution

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Position | Role | Date of Issue | Version |
| Mark Maxwell | DIO | Reviewer | 12/06/18 | 0.1 |
| Philip Gilmore | DPO | Reviewer | 21/06/18 | 0.2 |

Sign off

|  |  |
| --- | --- |
| Approver:  | Departmental Board |
| Signature: (digital) | [insert signature] |
| Date approved:  | 29 August 2018 |

**Contents**

[Introduction 1](#_Toc521920953)

[Objectives 4](#_Toc521920954)

[Policy Statement 5](#_Toc521920955)

[Data Protection Principles 6](#_Toc521920956)

[Data Protection Impact Assessments (DPIA) 7](#_Toc521920957)

[Rights of the Data Subject 8](#_Toc521920958)

[Departmental Privacy Statement 8](#_Toc521920959)

[Lawful basis for processing 9](#_Toc521920960)

[Data Sharing 10](#_Toc521920961)

[Data Processors 11](#_Toc521920962)

[Data Breach Management 11](#_Toc521920963)

[Notification Requirements 12](#_Toc521920964)

[Implementation 12](#_Toc521920965)

[The Role of Information Management Branch 13](#_Toc521920966)

[The Role of Business Areas 13](#_Toc521920967)

[The Role of the Data Protection Officer 14](#_Toc521920968)

[Acronyms / Glossary of Terms 16](#_Toc521920969)

[Appendix 1 17](#_Toc521920970)

[Appendix 2 (Special Category Data) 21](#_Toc521920971)

[Appendix 3 (Criminal Convictions / Offence Data) 23](#_Toc521920972)

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.
2. 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 etc.
3. The [Freedom of Information Act 2000](http://www.legislation.gov.uk/ukpga/2000/36/contents) and the [Environmental Information Regulations 2004](http://www.legislation.gov.uk/uksi/2004/3391/contents/made) determines the disclosure of the majority of information held by the department, including personal information relating to third parties.
4. The [Data Protection Act 2018](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf) implements the EU [General Data Protection Regulation](https://gdpr-info.eu/) (GDPR) and controls how personal information must be treated. Personal data is defined in the GDPR as:

*“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.”*

1. Some of the personal data processed by the Department can be more sensitive in nature and therefore requires a higher level of protection. The General Data Protection Regulations refers to the processing of these data as ‘special categories of personal data’.
2. Special category data is about an individual’s:
* race;
* ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* genetic data;
* biometric data (where this is used for identification purposes);
* health data;
* sex life; or
* sexual orientation.
1. The Department recognises that processing special category data could present a greater risk to an individual’s rights and freedoms and needs more protection. Information relating to criminal convictions and offences also requires a higher level of protection and is covered by Part 3 of the Data Protection Act 2018 which implements the EU Law Enforcement Directive.
2. The Data Protection Act 2018 and the General Data Protection Regulations enhance the rights of data subjects and ensures that any processing of personal data is compliant with the six principles.
3. The Data Protection Act 2018 is intended to ensure 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.
4. Every year the department deals with a number of information access and data protection requests involving personal information. The Information Commissioner, 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.
5. The ICO has authority to take enforcement action against those which do not comply. Organisations in breach of the General Data Protection Regulation can be fined up to 4% of annual global turnover or €20m. 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

1. The objective of the Data Protection Policy Statement is to show the Department’s commitment to comply with the General Data Protection Regulation and the Data Protection Act 2018, in relation to the following:
2. 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 utilising the guidance available to them on the Department’s Intranet site, the Information Commissioner’s website and from the Department’s Data Protection Officer at dataprotectionofficer@daera-ni.gov.uk.

.

Policy Statement

1. 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 2018 and the General Data Protection Regulation and endorses their requirements.
2. 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.
3. 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 implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of the legislation.
4. In the case of personal information relating to current members of staff, NICS HR is the Controller for this information and will be required to act in accordance with the legislation. There are some circumstances where line managers may retain local HR information that is not required or held by either HRConnect or NICSHR, for example records of informal discussions with members of staff, flexi sheets, job descriptions, evidence to assist with completing annual performance appraisal etc. This is not a definitive list, but illustrates the type of information that you, as a line manager, may need to retain. This information should be retained securely and only for as long as there is a business requirement to hold it. You should not be holding on to personal data about your staff for administrative convenience, or just in case it might be useful.

Data Protection Principles

1. Article 5(1) of the [General Data Protection Regulation](https://gdpr-info.eu/) requires that personal data shall be:
2. processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);
3. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);
4. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
5. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
6. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the [General Data Protection Regulation](https://gdpr-info.eu/) in order to safeguard the rights and freedoms of individuals (‘storage limitation’); or
7. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
8. Article 5(2) adds that the controller shall be responsible for, and be able to demonstrate compliance with Article 5(1) otherwise known as the “Accountability” principle.
9. These principles lie at the heart of the Department’s approach to processing personal data. The Department will seek, through appropriate management and strict controls, to comply with these principles.

Data Protection Impact Assessments (DPIA)

1. The General Data Protection Regulation introduces a requirement to complete a Data Protection Impact Assessment before carrying out any types of processing **likely to result in high risk** to individuals’ interests.
2. A Data Protection Impact Assessment screening exercise is a process to help business areas make an initial evaluation of the probable level of risk involved in their planned process and therefore minimise the data protection risks of any project. Should the screening exercise indicate a higher risk process being undertaken, it is now a statutory requirement that a full Data Protection Impact Assessment must be undertaken before further development of the process can proceed.
3. Business areas should follow the Departmental Guidance available on the intranet and in particular undertake screening exercises at an earliest stage possible.
4. If a Data Protection Impact Assessment identifies a high risk that a business area cannot mitigate it must consult with the Departmental Data Protection Officer who will provide advice. The Departmental Data Protection Officer may need to consult with the ICO who will provide written advice. This advice can take up to 14 weeks and this timeline reinforces the need for the timely carrying out of Data Protection Impact Assessment’s.

Rights of the Data Subject

1. Article15 of the General Data Protection Regulation sets out the rights of access to personal information held by DAERA that data subjects have. Individuals can obtain from DAERA confirmation as to whether or not we are processing data concerning them, and if so access to that information (unless an exemption applies) and:
* the purpose of the processing;
* the categories of personal data concerned;
* the recipients or categories of recipient to whom the data has been disclosed and in particular recipients in third countries or international organisations;
* the envisioned period of time the personal data will be held for, or if not possible, the criteria used to determine the period;
* their right to request from DAERA rectification or erasure of data or restriction on the processing of personal data concerning the data subject or to object to the processing;
* the right to lodge a complaint with the Information Commissioner’s Office;
* if the personal information was not supplied by the data subject, the source of that information; and
* the right to question decision-making and profiling based on automated means.

Departmental Privacy Statement

1. The Department’s Privacy Statement (**Appendix 1**) provides an overarching guide to how the Department will process the personal information it holds.
2. It has been created to identify the range of circumstances where the Department collects personal information so that data subjects know how the Department intends to process their personal details.
3. The Department recognises that there may be occasions where individual business areas will need to tailor and create task specific privacy notices. When doing so, business areas should contact the Departmental Data Protection Officer for further advice.

Lawful basis for processing

1. The Department must have a valid lawful basis in order to process personal data. There are six lawful bases and the most appropriate to use will depend on the purpose and relationship with the individual. They are set out in Article 6 *(Lawfulness of processing)* of the General Data Protection Regulation and at least one of these must apply whenever you process personal data.
2. If the Department is processing special category data, it needs to identify **both** a lawful basis for processing **and** a special category condition for processing. These are listed in Article 9(2) (*Processing of special categories of personal data)* of the General Data Protection Regulation (**Appendix 2**).
3. When processing special category or criminal offence data, the Department should document both the lawful basis for processing and the relevant separate condition so that it can ably demonstrate compliance and accountability. A list of the requirements of both articles is attached at **Appendix 2**.
4. If the Department is processing data about criminal convictions, criminal offences or related security measures, the Department needs both a lawful basis for processing and a separate condition for processing in compliance with Article 10 (**Appendix 3**).

Data Sharing

1. It is particularly important to note the need to have proper Data Sharing Agreements in place 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.
2. Data subjects are entitled to be informed at the time personal information is collected how it will be used and any wider use would be in contravention of the Data Protection Act 2018. The DAERA Privacy Statement sets out how personal information is to be processed by the Department and it is available on the Departmental website.
3. The Data Protection Act 2018 requires the Information Commissioner to prepare a code of practice for this purpose and the Department should adhere to its provisions.
4. The Privacy Statement also 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 2018 and Freedom of Information legislation.
5. The Department will provide bulk personal information to another public body where there is a legitimate and lawful reason for doing so. Any business area receiving requests for personal information of this type should consult the Departmental Data Protection Officer before taking any further action.
6. Sometimes the Department is required to provide personal information in order to facilitate, for example, tax assessment, fraud investigation or criminal investigations. Under these circumstances the Department will provide specific information about an individual or number of individuals who are under investigation.
7. The Department often receives Environmental or 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 Data Protection Principles are applied fairly and legislative requirements intended to safeguard personal information are met.

Data Processors

1. 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.
2. This applies equally when it is being processed by others on the Department’s behalf. 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.
3. Security measures must be at least equivalent to those we would apply if doing the job ourselves.

Data Breach Management

1. In the event of any breach involving personal data which is likely to result in a risk to the rights and freedoms of individuals it must be reported to the Departmental Data Protection Officer as soon as you are aware of it. The Data Protection Officer then must report it to the Information Commissioner within 72 hours. Business areas should ensure that they act in accordance with the DAERA Data Breach Management Plan.
2. The Department will act in accordance with the Information Commissioner’s advice on the four elements of a breach management plan which are:-
* Containment and recovery;
* Assessment of ongoing risk;
* Notification of breach;
* Evaluation and response.

Notification Requirements

1. Under the General Data Protection Regulation, organisations that determine the purpose for which personal data is processed (controllers) must pay the ICO a data protection fee unless they are exempt.
2. The new data protection fee replaces the requirement to ‘notify’ (or register). The ICO has the power to enforce the 2018 regulations and to serve monetary penalties on those who refuse to pay their data protection fee.
3. The ICO will publish details of all data controllers who pay the fee and their Data Protection Register is made available to the public on the Information Commissioner’s Website.

Implementation

1. Responsibility for delivering the actions relating to the rights of the data subject rests with both Information Management Branch and business areas. Information Management Branch plays a central role in terms of raising awareness, providing advice on managing requests and the handling of internal reviews.
2. It is the responsibility of Information Asset Owners (IAO) / Heads of Branch 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 legislative requires.
3. IAOs at all levels, are responsible and accountable for the information held and processed by their business area. IAOs should ensure their Information Asset Register (IAR) accurately reflects all assets involved in the processing of personal data alongside the action taken to mitigate against the potential for data breaches.
4. All civil servants, regardless of grade, have a legal duty to protect and maintain the confidentiality of personal data held by their Department.

## The Role of Information Management Branch

1. Specific actions to be taken by IMB include:
	* providing support to the Data Protection officer in their role;
	* making available to business areas the advice and assistance they require to comply with the legislation. Publicising this policy, publishing information on the intranet, signposting staff to relevant and most up to date training available and liaising with business areas when they are responding to information access requests;
	* confirming with business areas on an regular basis that their IAOs have been trained and are content with the data processing procedures they have in place;
* coordination of a range of Information Assurance exercises to satisfy the accountability principle within GDPR; and
* handling the investigation of related complaints.

## The Role of Business Areas

1. Specific actions to be taken by business areas include:
* ensuring relevant staff are trained in protecting personal information and are familiar with the requirements of the General Data Protection Regulation and the Data Protection Act 2018;
* ensuring that relevant procedures are in place and followed by staff;
* conduct Data Protection Impact Assessments when necessary;
* responding promptly to the range of Information Assurance activities;
* ensuring all personal information is accessible in the event that it is requested by a data subject;
* take account of the DAERA Data Protection Officer’s advice and the information they provide on our data protection obligations;
	+ ensuring requests for personal information are dealt with under the timelines set within the relevant statutory framework;
	+ ensuring that personal information is held no longer than necessary in the appropriate repository, kept secure, 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 Data Protection Act 2018 and the Department’s retention and disposal schedule.
	+ ensuring appropriate techniques like encryption are applied when necessary;
	+ reporting any breach of personal data to the Data Protection Officer as soon as you are aware of it;
	+ ensure that all laptops are encrypted and that staff who need to use portable media devices follow the procedures as laid down in DAERA’s Information Security Standards.
	+ ensuring that data protection procedures are documented (for example, in office procedures manuals and job descriptions);
* reviewing internal procedures at least annually;
	+ liaising with Information Management Branch about any data protection issue they are unsure about.

The Information Asset Owner and the Main Decision Maker within each business area have specific responsibility for ensuring these aspects are taken forward.

## The Role of the Data Protection Officer

1. The DAERA Data Protection Officer is tasked with monitoring compliance with the General Data Protection Regulation and other data protection laws, or data protection policies, awareness-raising, training, and audits.
2. Under this Data Protection Policy, overall responsibility for complying with the requirements of the General Data Protection Regulation and Data Protection Act 2018 rests with the Permanent Secretary.
3. In practice, many of the functions are devolved to the Data Protection Officer who is expected to oversee compliance in conjunction with Heads of Branches.
4. The Data Protection Officer and other staff in Information Management Branch are available to advise on issues which arise.
5. All managers and staff in Business areas, including Agencies, that process personal information should ensure that job descriptions and Personal Performance Agreements accurately reflect these responsibilities and, if necessary, Personal Development Plans.
6. 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 three yearly intervals.

Acronyms / Glossary of Terms

| **Acronym/Abbreviation/Term** | **Meaning** |
| --- | --- |
| DAERA | Department of Agriculture, Environment and Rural Affairs |
| Data controller | a person or organisation determining how and why information is processed. |
| Data subject | an individual to whom personal information relates |
| DIO | Department Information Officer. The civil servant responsible for providing support and guidance to the Department on information management matters. |
| DRO | Department Records Officer |
| DPA 1998 | Data Protection Act 1998 |
| DPA 2018 | Data Protection Act 2018 |
| DPIA | Data Protection Impact Assessment |
| DPO | Data Protection Officer – Responsible for monitoring DAERA’s compliance with the existing legislative framework |
| EIR | Environmental Information Regulations 2004 |
| FOI | Freedom of Information Act 2000 |
| GDPR | General Data Protection Regulation |
| HPRM | Hewlett Packard Records Management. The NICS wide records management system (Records NI). |
| IAO | Information Asset Owner. The civil servant who owns responsibility for all aspects of managing a DAERA information asset. |
| ICO | Information Commissioners Office. The UK independent regulatory body concerned with data privacy issues. |
| IMB | Information Management Branch at DAERA |
| ISMS | DAERA’s Information Security Management System |
| NICS | Northern Ireland Civil Service. The umbrella term used to describe the organisation responsible for the operation of Her Majesty’s Government in Northern Ireland. |
| Privacy Notice | a statement of how the Department may process personal information |

Appendix 1

**DAERA Privacy Statement**

**Contacts**

Data Control Name

Department of Agriculture, Environment and Rural Affairs
Ballykelly House,
111 Ballykelly Road,
Ballykelly,
Limavady,
BT49 9HP

**DAERA Data Protection Officer (DPO)**

Telephone: 028 9052 4316
Email: dataprotectionofficer@daera-ni.gov.uk

A hard copy of this Privacy Statement is available to download from the following page:

* [DAERA Privacy Statement document](https://www.daera-ni.gov.uk/publications/daera-privacy-statement-document)

**Why are you processing my personal information?**

The Department takes data protection, freedom of information and environmental information issues seriously. It takes care to ensure that any personal information received from you is dealt with in a way which complies with the requirements of the General Data Protection Regulations (2016). This means that any personal information you supply will be processed principally for the purpose for which it has been provided.

However, the Department is under a duty to protect the public funds it administers, and to this end may use the information you have provided for this purpose. It may also share this information with other bodies responsible for the audit or administration of public funds, in order to prevent and detect crime.

In addition, the Department may also use it for other legitimate purposes in line with the General Data Protection Regulations, Freedom of Information Act 2000 and Environmental Information Regulations 2004.

These include:

* administration of the Common Agricultural Policy and other aid schemes
* administration of the Common Fisheries Policy
* the production and safety of food;
* management of land and other environmental controls;
* animal health and welfare;
* statutory schemes and obligations in the areas of plant health and crop certification;
* occupational health and welfare;
* regulatory and natural resources policy;
* environmental policy;
* legislation relating to the Northern Ireland Environmental Agency;
* the prevention and detection of fraud or maladministration (e.g. The Comptroller & Auditor General and HM Revenue & Customs);
* compilation of statistics;
* disclosure to other organisations when required by law to do so;
* disclosure under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 where such disclosure is in the public interest;
* administration of UK wide schemes on behalf of the Department for the Environment, Food and Rural Affairs in Great Britain;
* business development and knowledge advisory service for farmers, growers and food processors;
* for corresponding with you in connection with the above activities;

**Where do you get my personal data from?**

The Department will collect your information primarily from applications for services and subsequent information that you provide to us, as the data subject, in relation to the provision of these services. The Department may also collect additional information from other agencies that is necessary to provide the services requested.

The Department will also maintain and update your data with any information you subsequently share with us in order to ensure your data is factual, accurate and up-to-date.

**Do you share my personal data with anyone else?**

Data sharing takes place for legitimate reasons, to support the business purposes for which it was supplied. If we need to share your personal data, it will be done so under contract which will require the processor to protect the data and act only in regard to DAERA business purposes.

**We may share your data with:**

* enforcement agencies for the prevention or detection of crime;
* tax and customs authorities, when requested by them to do so;
* selected third party processors who we use for processing applications or for making payments to you;
* NI Direct;
* third party ICT systems to support contractors who maintain our ICT systems which hold your personal data.

**Do you transfer my personal data to other countries?**

Sometimes it may be necessary to transfer personal information overseas. When this is needed, information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the General Data Protection Regulations (2016).

**How long do you keep my personal data?**

We will retain your data only for as long as necessary to comply with legislation, and/or where there is a business need to do so (i.e. for the administration of your application and/or payment). Your data will be kept in line with our Retention and Disposal Schedule.

**Changes to this Privacy Statement**

We will make changes to this statement from time to time, particularly when we change how we use your information or the services we provide. You can always find an up-to-date version of this notice on our website at the link below:

* [DAERA Privacy Statement document](https://www.daera-ni.gov.uk/publications/daera-privacy-statement-document)

You can also contact the DAERA Data Protection Officer should you require further information (contact details given below, should you require further information). This privacy statement was last updated on 1 May 2018.

**What rights do I have?**

|  |  |
| --- | --- |
| The right to be informed | The right of access |
| The right to rectification | The right to erasure |
| The right to restrict processing | The right to data portability |
| The right to object | Rights in relation to automated decision making and profiling |

Should you require any further information on your rights in relation to the data we collect or process, please contact the DAERA Data Protection Officer in the first instance.

**How do I complain if I am not happy?**

If you are unhappy with any aspect of this privacy statement, or how your personal information is being processed, please contact DAERA Data Protection Officer at:

Department of Agriculture, Environment and Rural Affairs

Ballykelly House,

111 Ballykelly Road

Ballykelly,

LIMAVADY

BT49 9HP

Telephone: 028 9052 4316

Email: dataprotectionofficer@daera-ni.gov.uk

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner’s Office (ICO):

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

Email: casework@ico.org.uk

Website:[https://ico.org.uk/global/contact-us/](https://ico.org.uk/global/contact-us/%22%20%5Ct%20%22_blank%22%20%5Co%20%22external%20link%20opens%20in%20a%20new%20window%20/%20tab)

Appendix 2 (Special Category Data)

The conditions listed in Article 9(2) of the [General Data Protection Regulation](https://gdpr-info.eu/) are:

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Staff should read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

* Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (g), (i) and (j).
* Schedule 1 Part 2 contains specific ‘substantial public interest’ conditions for Article 9(2)(h).

In some cases you must also have an ‘appropriate policy document’ in place to rely on these conditions.

Appendix 3 (Criminal Convictions / Offence Data)

**Article 10 states:**

“Processing of personal data relating to **criminal convictions and offences** **or related security measures** based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

This means you must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill. We will publish more detailed guidance on the conditions in the Bill once these provisions are finalised.

Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.