information commissioner
Barrantagh Fysseree

# Getting ready for the new data protection laws

## A guide for small businesses, charities and voluntary organisations

# Your business and the new data protection laws

Data protection and privacy laws are being strengthened throughout the world in response to the ever increasing use of technology and the threats such processing poses to individuals. In the European Union new law, known as the EU General Data Protection Regulation (GDPR), comes into full force on 25 May 2018.

The Isle of Man is introducing new data protection laws similar to the GDPR which are also expected to come into force in May 2018. If you process personal data as part of your business, charity or other organisation including clubs and societies, then these laws apply to you.

This guide is intended to assist smaller businesses, voluntary organisations and charities that do not process large amounts of personal data and do not have access to expert resources to understand their obligations and prepare for the new laws. The GDPR is an evolution of the existing law. If you are already complying with the Data Protection Act 2002, and have good data protection policies in place, then you are already on the way to being prepared for the GDPR.

It is important to remember that:

- Information concerning Customers, Staff, Volunteers and Members is **'personal data'.**
- Simply storing that personal data either electronically or in hardcopy constitutes **'processing'.**

# Glossary of terms

This guide uses certain terms such as personal data, data subject, controller and processor. The Glossary at the end of this guide provide a brief explanation of these terms. Full definitions can be found in our *"Closer Look at Definitions"* guide at:
https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/compliance-resources/gdpr-guidance/:

# A risk based approach

The new laws advocate a risk based approach requiring for example *"appropriate organisational and technical measures to ensure a level of security appropriate to the risk."*

When your business or organisation obtains, stores or otherwise processes personal data, the individuals whose personal data you are processing are exposed to risk, for example if the personal data was to be misused or lost then a risk of identity theft or fraud, financial loss, damage to reputation, loss of professional confidentiality, etc., may arise.

To mitigate those risks it is important that you take steps to ensure that the personal data is processed lawfully and securely.

The level of risk depends upon a number of factors, for example, where processing is complex, or involves special category data, such as health data, the risk posed is considerably greater than simply processing a customer's name and address.

A risk assessment of the processing of personal data by your business or organisation should be carried out to determine the complexity and scale of processing, the sensitivity of the data processed and the appropriate level of protection required for that data. A risk assessment will also improve awareness in your organisation of the issues, including the potential damage that may result to your organisation, if personal data is misused or lost.

**Maintaining records of your processing, including a risk register, can allow you to identify and mitigate future risks, as well as demonstrate compliance in the event of a regulatory investigation or audit.**

# Key Concepts

## The Principles

When processing personal data all businesses and organisations must follow the following six principles:-

**Lawfulness, fairness and transparency**
Personal data shall be processed lawfully, fairly ***and in a transparent manner in relation to the data subject***

**Purpose limitation**
Personal data shall be collected for specified, ***explicit*** and legitimate purposes and not further processed in a manner that is incompatible with those purposes

**Data minimisation**
Personal data shall be adequate, relevant and ***limited to what is necessary*** in relation to the purposes for which they are processed

**Accuracy**
Personal data shall be accurate and, where necessary, kept up to date

**Storage limitation**
Personal data shall be 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

**Integrity and confidentiality**
Personal data shall be 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

For more detailed information about these principles, see our *"Closer Look at Principles"* guide at:
https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/compliance-resources/gdpr-guidance/

## Lawfulness

In order to process personal data you must have a lawful basis to do so. In summary these are:-

- consent of the individual;
- performance of a contract;
- compliance with a legal obligation;
- necessary to protect the vital interests of a person;
- necessary for the performance of a task carried out in the public interest; or
- in the legitimate interests of the business, company, or organisation, except where those interests are overridden by the interests or rights and freedoms of the data subject.

If your processing involves ***special categories of data*** then you may only process that data if:-

- you have the explicit consent of the individual;

or, the processing is necessary:-

- to comply with employment, social security or social protection legal obligations;
- to protect the vital interests of an individual where consent cannot be obtained;
- for the legitimate activities of an association or not-for-profit body where the processing relates solely to the members of the body;
- for legal purposes;
- for reasons of substantial public interest, provided for by law;
- for the purposes of preventive or occupational medicine,
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest.

# Fairness and Transparency

You must provide individuals with information about the use of their personal data in clear, concise and plain language. This could be achieved for example by notices on your website or signs at points of sale.

The information to be provided, and when, depends upon a number of factors. In general the information must include:-

- your identity and contact details;
- where applicable the contact details of your Data Protection Officer;
- the purposes of processing and the legal basis for processing (including the legitimate interest pursued by the controller if applicable);
- the identity of any third party to whom the data may be disclosed; and
- how the data will be protected.

You may also have to explain:-

- how long the data will be kept;
- the rights of the individual, including access, rectification, objection and portability;
- the right to withdraw consent where processing is based on consent;
- the right to complain to the Information Commissioner;
- whether the data is required due to a statutory or contractual obligation; and
- what the consequences to the individual are of not providing the information.

For more detailed information see our *"Closer Look at Transparency"* guide at:
https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/compliance-resources/gdpr-guidance/
and the UK Information Commissioner's "Privacy notices, transparency and control " pages at:
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

## Security of Processing

You are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk the processing poses to an individual.

In determining the technical and organisational measures required you need to take into account the risk posed by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data that you process.

You are required to regularly test, assess and evaluate the effectiveness of these technical and organisational measures, keeping records to demonstrate that you have done so.

## Data breaches

Unless a data breach is unlikely to result in a risk to an individual, your business or organisation must report any data breach to the Information Commissioner with 72 hours of becoming aware of that breach. In doing so you will be required to describe:-

- the nature of the breach, including the approximate number of data subjects involved and the number of personal records concerned,
- the likely consequences or adverse effects of the breach to the individual,
  and
- the measures taken or proposed to be taken to address the breach and mitigate its adverse effects.

You may also be required to inform every data subject of the breach without undue delay.

## Data Protection Officer

You will also need to determine whether you require a Data Protection Officer. For more detailed information see our *"Closer Look at Data Protection Officer"* guide at:
https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/compliance-resources/gdpr-guidance/

# Rights and Remedies

Data Subjects have a number of rights and remedies. In most cases these rights are **free to exercise** and must be complied with within **one month** of receiving the request.

In summary the rights are:-

- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object to processing

while remedies include:-

- Right to lodge a complaint with a supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to compensation from controllers and processors

For more detailed information see our *"Closer Look at Rights and Remedies"* guide at:
https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/compliance-resources/gdpr-guidance/

# Steps to compliance

- Identify what personal data you process. This can be achieved by using our *"Know Your Data: Mapping the 5 W's"* guide which can be found at: https://www.inforights.im/media/1271/gdpr_part-1_toolkit_mapping_may2016.pdf

- Review that processing (see questionnaires below) and where necessary :-
    - ❖ identify your purposes for processing personal data;
    - ❖ whether the personal data you process includes any special categories of personal data;
    - ❖ identify the lawful basis for all processing of personal data;
    - ❖ ensure that you are only processing the minimum amount of personal data necessary for the identified purpose;
    - ❖ ascertain how you confirm that the personal data obtained is accurate and where necessary ensure there are processes in place to keep that data accurate; and
    - ❖ establish and justify the periods for retaining that data.

- Determine how you will provide information to the various data subjects, including staff, volunteers, customers, members, etc., which explains why you need to process their personal data, what you will use that data for, including who it may be disclosed to, and how long you will keep that data.

- Implement appropriate technical and organisational measures to ensure personal data (whether held electronically or on paper) is securely stored and safely destroyed or deleted when no longer required.

- Ensure there are processes in place to facilitate requests from data subjects seeking to exercise their rights.

- Where appropriate, have up-to-date policy/procedure documents that detail how your business or organisation is meeting its data protection obligations.

- Determine whether you require a Data Protection Officer (DPO).

# Questionnaires

## Personal Data You Process

The following should have been identified:

| Categories of data subjects | Personal data included in each data category | Source of personal data | Purposes for which personal data is processed | Lawful basis for each processing purpose (non-special categories of personal data) | Special categories of personal data | Lawful basis for processing special categories of personal data | Retention period | Any actions required for compliance? |
|---|---|---|---|---|---|---|---|---|
| *For example:- current staff data; retired staff data; client data (sales information); marketing database; CCTV* | *For example:- name, address, bank account, sales history, online browsing history, video images.* | *For example:- collected directly from data subject; obtained from third party (Identify third party data controller).* | *For example:- HR, accounts, marketing, research, product development, system integrity.* | *For example:- consent, contract, legal obligation, etc.* | *If special categories of personal data are processed identify the type of data.*<br><br>*For example:- health, genetic, biometric data* | *For example:- explicit consent, legal requirement.* | *For each category of personal data, list the period for which the data will be retained and why.*<br><br>*For example:- five years as required by AML/KYC legislation* | *For example:- deleting existing personal data where no legitimate purpose for continued retention has been identified.* |

## The Principles

| Principle | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| Lawfulness, fairness and transparency | **Fairness and Transparency**<br>*see specific section below* | | | |
| | **Lawfulness**<br>Have you identified the lawful basis for each purpose for which you process personal data? | | | |
| | **Lawfulness - Consent.**<br>Have you reviewed your organisation's mechanisms for obtaining consent to ensure that it is freely given, specific and informed? | | | |
| | **Lawfulness - Consent.**<br>Are procedures in place to record and demonstrate that an individual has consented by way of a clear indication to the processing of their data? | | | |
| | **Lawfulness - Consent.**<br>Are there procedures in place to permit an individual to withdraw their consent to that processing? | | | |
| | **Lawfulness - Consent.**<br>If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected? | | | |

| Principle | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| | **Lawfulness – Consent – children**<br>Are procedures in place to verify age and get valid consent of a parent or guardian, where required? | | | |
| | **Lawfulness - Legitimate interests.**<br>Can you demonstrate that reliance upon this legal basis is appropriate and:-<br>• there is a valid legitimate interest;<br>• the data processing is strictly necessary in pursuit of that legitimate interest; and<br>• the processing is not prejudicial to or overridden by the rights of the individual? | | | |
| | **Lawfulness - Legitimate interests.**<br>Note: a public authority cannot rely upon legitimate interests. | | | |
| Purpose limitation | Is personal data only used for the purposes for which it was originally collected? | | | |
| | Is the personal data disclosed or shared with any other party? If so can you identify every other party? | | | |
| Data minimisation | Is the personal data limited to what is necessary for the purposes for which it is processed? | | | |

| Principle | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| Accuracy | Are procedures in place to ensure personal data is kept up to date and accurate and any necessary changes are made without delay? | | | |
| | Where personal data are obtained from a third party, are there processes in place to verify the accuracy of that data before further processing occurs? | | | |
| Storage Limitation | Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected? | | | |
| | Is your business subject to rules that require a minimum retention period (e.g. tax/NI returns, AML/KYC records)? | | | |
| | Do you have procedures in place to ensure data is destroyed securely, in accordance with your retention policies? | | | |
| Integrity and Confidentiality | *See specific section below* | | | |

# Fairness and Transparency

| Question | Yes | No | Comment/Action |
|---|---|---|---|
| Are employees, volunteers, members and customers fully informed of how you use their data in a concise, transparent, intelligible and easily accessible method using clear and plain language? ***(Transparency)*** | | | |
| Where personal data is collected directly from the data subject, how is the transparency information provided? | | | |
| Where personal data is **not** collected from the data subject but from a third party, how is the transparency information provided? | | | |
| Has information on how your business or organisation facilitates data subjects to exercise their rights been made available in an easily accessible and readable format? | | | |
| Are procedures in place to proactively inform data subjects of their rights when your business or organisation is directly engaged with the data subject and processing their personal data, for example when providing a service, a retail sale or CCTV monitoring? | | | |

# Integrity and Confidentiality

| Question | Yes | No | Comment/Action |
|---|---|---|---|
| Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them? | | | |
| Do you have a documented security policy that describes the technical, administrative and physical safeguards for personal data? | | | |
| Have you designated an individual with responsibility for information security including the investigation of security incidents and breaches? | | | |
| Do you have documented processes and procedures for investigating and resolving security related complaints and issues? | | | |
| Can access to personal data be restored in a timely manner in the event of an incident? | | | |
| Is personal data systematically destroyed, erased, or anonymised in accordance with retention policies when no longer required? | | | |
| Are procedures in place to ensure that there is no unnecessary or unregulated duplication of records? | | | |
| If you process special category data, such as health data, do you employ encryption techniques to transfer, store, and receive such data? | | | |

## Data Breaches

| Question | Yes | No | Comment/Action |
|---|---|---|---|
| Does your business or organisation have a documented data breach response plan? | | | |
| Are all staff aware how, and to whom within the organisation, a data breach must be reported? | | | |
| Are all data breaches fully documented? | | | |
| Are there procedures in place to notify the Information Commissioner of a data breach? | | | |
| Are there procedures in place to notify data subjects of a data breach when necessary? | | | |
| Where your business discloses or shares personal data with other controllers and processors are there procedures in place to deal with any data breach? | | | |
| Are plans and procedures regularly reviewed? | | | |

# Data Protection Officers

| Question | Yes | No | Comment/Action |
|---|---|---|---|
| Are you required to appoint a Data Protection Officer (DPO)? | | | |
| If you have determined that you are not legally required to appoint a DPO, have you documented the reasons why? | | | |
| Where a DPO is appointed, are the tasks and duties documented and reporting lines in place? | | | |
| Have you published the contact details of your DPO so that customers and staff are able to contact them? | | | |
| From May 2018, have you informed the Information Commissioner of your DPO's contact details? | | | |

## Rights and Remedies

| Right | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| General | Where a DPO has not been designated, have you identified who will deal with, and respond to, an individual exercising any of their rights? | | | |
| | Has your organisation established processes to fully respond within **one month** to an individual exercising any of their rights? | | | |
| Access to personal data | Is there a documented policy/procedure for handling requests to access personal data? | | | |
| Deletion and rectification | Are there controls and procedures in place to allow personal data to be deleted or rectified when necessary? | | | |
| Right to restriction of processing | Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing? | | | |
| Data portability | Are procedures in place to provide individuals with their personal data in a structured, commonly used and machine readable format? | | | |

| Right | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| Right to object to processing | Have you made individuals aware of their right to object to certain types of processing such as direct marketing or where the legal basis of the processing is legitimate interests or necessary for a task carried out in the public interest? | | | |
| | Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing? | | | |
| Profiling and automated processing | Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision? | | | |

## Controllers and Processors

| Question | Yes | No | Comment/Action |
|---|---|---|---|
| Have you reviewed contracts and agreements with suppliers and other third parties that process personal data on your behalf to ensure new requirements have been included? | | | |

# Transfers outside the Isle of Man

| Transfers | Question | Yes | No | Comment/Action |
|---|---|---|---|---|
| **International data transfers** | Is personal data transferred outside the Island? | | | |
| | Does this include any special categories of personal data? | | | |
| | What is the purpose(s) of the transfer? | | | |
| | Who is the transfer to? | | | |
| | What is the legal basis for the transfer, e.g. EU Commission adequacy decision; standard contractual clauses.<br><br>Are these documented? | | | |
| Transparency | Are data subjects fully informed about any intended international transfers of their personal data? | | | |

# Glossary of terms

**GDPR:** EU General Data Protection Regulation (2016/679).

**Personal Data:** Information relating to a living individual who is, or can be, identified by that information, including data that can be combined with other information to identify an individual. This can be a very wide definition, depending on the circumstances, and can include data which relates to the identity, characteristics or behaviour of an individual or influences the way in which that individual is treated or evaluated.

**Processing**: means performing any operation or set of operations on personal data, including:

a. Obtaining, recording or keeping data;
b. Organising or altering the data;
c. Retrieving, consulting or using the data;
d. Disclosure, which includes publication, of the data to a third party; and
e. Erasing or destroying the data.

**Controller**: A Controller is the person or organisation who decides the purposes for which, and the means by which, personal data is processed. The purpose of processing data involves 'why' the personal data is being processed and the 'means' of the processing involves 'how' the data is processed.

**Processor:** A person or organisation that processes personal data on the behalf of and under the instructions of a controller.

**Data Subject:** The individual the personal data relates to.

**Data Protection Impact Assessment (DPIA):** A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and as far as possible setting how to minimize those risks. DPIAs are important tools for negating risk, and for demonstrating compliance, including ongoing compliance. (For more guidance see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

**Retention Policy:** A policy that sets out how long you hold various categories of personal data.
In general, personal data must not be kept for longer than necessary for the purposes for which the data are processed. A retention policy identifies how long each category of personal data is retained and may also set out how that data will be securely destroyed or deleted at the end of the retention period. A retention period may be due to a legal requirement such as tax and national insurance returns.

**Special Categories of personal data:** Personal data 'which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

**Consent:** Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she signifies agreement to the processing of their personal data.