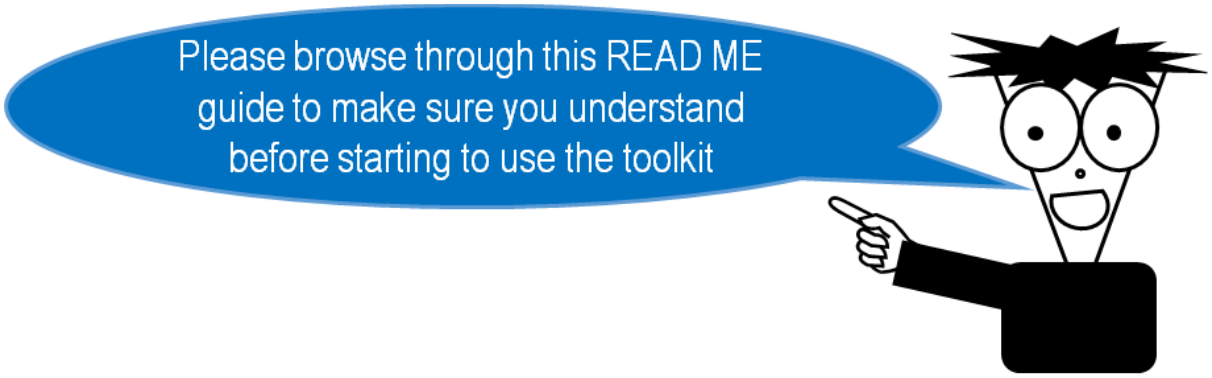
# GDPR Toolkit

## DATA PROTECTION POLICY

# GDPRToolkit

**INTRODUCTION**
Please read the READ ME User Guide first to make sure you know and understand the need to add, amend, or delete in order to reflect your people, processes and technologies as well as the data you hold and the jurisdiction(s) you operate in.




The READ ME User Guide will you help navigate around the GDPR-Toolkit and identify what you need to do for your organisation.

**DISCLAIMER**
GDPR can be complicated and there are different laws in UK, EU, Jersey and Guernsey. Simply having Templates, Documents, Samples and Guidance does not make you compliant.

The reason for this disclaimer is that I cannot warrant or guarantee materials for every system or circumstance or jurisdiction and the client/user/recipient is obliged to review, test and where necessary customise or take advice to generally assert that they are satisfied before using this “live”.

If DIY isn’t for you, that’s OK. I’m rubbish at electrical work, plumbing or carpentry. Call an expert. There are many out there and data protection is too important for you, your organisation and the people who trust you with their data for you to get it wrong.

**SUPPORT**
For those organisations without the resources, skills or experience I can help with training or provide support to customise the documents to meet your particular needs. TimHJRogers@AdaptConsultingCompany.com

# GDPRToolkit

Contents



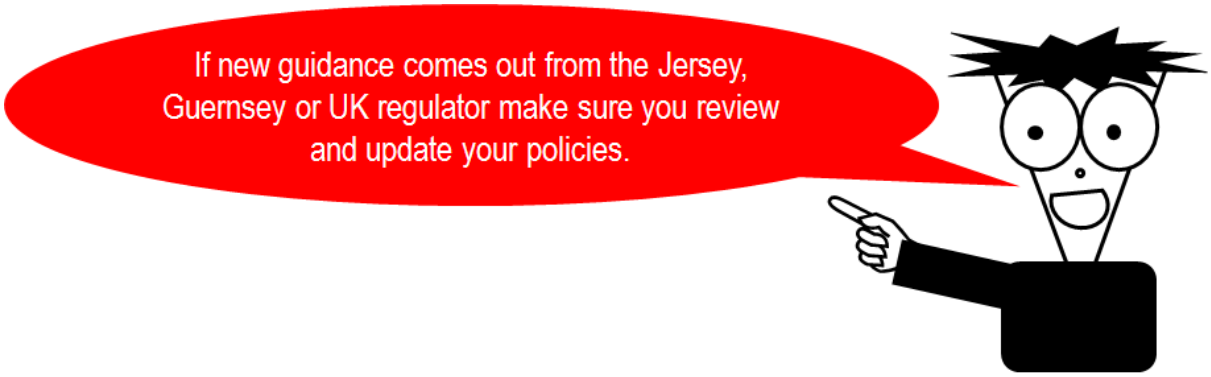
[Organisation name] needs to collect and use certain types of information in order to carry on our work, which includes

[ORGANISATION NAME]; [LIST OF TYPES OF INFORMATION RELEVANT TO DATA PROTECTION POLICY]; [DOCUMENT OWNER]; [AUTHOR]; [APPROVER];

This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Legislation

## 1. DATA PROTECTION LEGISLATION

These procedure base is based on guidance from the UK ICO and related to Data Protection (Jersey) Law 2018




https://www.jerseylaw.je/laws/enacted/Pages/L-03-2018.aspx
https://www.jerseylaw.je/laws/enacted/Pages/L-04-2018.aspx

## 2. DATA CONTROLLER

[Organisation name] is the Data Controller under the Data Protection Legislation, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

## 3. DISCLOSURE

[Organisation name] may share data with other organisations, but only in-so-far-as it is necessary for us to be able to operate and provide services.

[Organisation name] have Privacy Notices for each key service area and this sets out the basics. In some cases there may be additional documents - contract, agreement, terms - with more details specific to the person or service.

The Individual/Service User will be made aware how and with whom their information will be shared. There are circumstances where the law demands [Organisation name] to disclose data (including sensitive data) without the data subject's consent.

These include:

1. Carrying out a legal duty
2. Protecting vital interests of a Individual/Service User or other person
3. The Individual/Service User has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion

[Organisation name] regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. [Organisation name] intends to ensure that personal information is treated lawfully and correctly.

To this end, [Organisation name] will adhere to the Principles of Data Protection, as detailed in the Data Protection Legislation, and following the latest guidance generally available from the ICO website

Specifically, the Principles require that personal information:

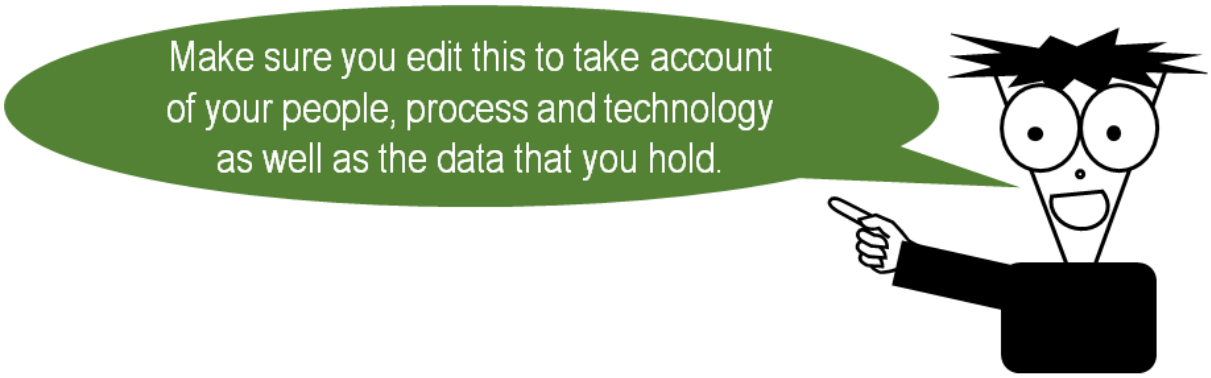
1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information, without the knowledge and agreement of the data-subject.

[Organisation name] will, through appropriate management and strict application of criteria and controls:

1. Observe fully conditions regarding the fair collection and use of information
2. Meet its legal obligations to specify the purposes for which information is used
3. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
4. Ensure the quality of information used

## 4. DATA COLLECTION




[Organisation name] will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form, or by mutual agreement (eg contract, terms-and-conditions, etc.)

[Organisation name] have a Privacy Notice and this sets out the basics. In some cases there may be additional documents - contract, agreement, terms - with more details specific to the person or service.

When collecting data, [Organisation name] will ensure that the Individual/Service User:

1. Clearly understands why the information is needed

2. Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
3. As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
4. Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
5. Has received sufficient information on why their data is needed and how it will be used

## 5. DATA RETENTION AND STORAGE

Information and records relating to service users will be stored securely and will only be accessible to authorised personnel.

We operate a records retention policy which sees the deletion, archive, return of documents at the point of their expire and in accordance with the policy and processes outlined in the records retention policy.

[Organisation Name] have a Records Management Policy and Data Retention Schedule to ensure Information will be stored for only as long as it is needed or required by statute, legislation or regulation and will be disposed of appropriately.

For contracts with the States of Jersey [Organisation Name] are bound by Freedom of Information FOI, and will act in accordance for States of Jersey Contracts.

We operate a information security policy systems which complies with Cyber Essentials principles

- Secure your Internet connection
- Secure your devices and software
- Control access to your data and services
- Protect from viruses and other malware
- Keep your devices and software up to date

It is [Organisation Name] responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

## 6. DATA ACCESS AND ACCURACY

All Individuals/Service Users have the right to access the information [Organisation Name] holds about them. [Organisation Name] will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, [Organisation Name] will ensure that:

1. It has a Data Protection Manager with specific responsibility for ensuring compliance with Data Protection
2. Everyone processing personal information understands that they are contractually responsible for following good data protection practice
3. Everyone processing personal information is appropriately trained to do so
4. Everyone processing personal information is appropriately supervised
5. Anybody wanting to make enquiries about handling personal information knows what to do
6. It deals promptly and courteously with any enquiries about handling personal information
7. It describes clearly how it handles personal information
8. It will regularly review and audit the ways it hold, manage and use personal information
9. It regularly assesses and evaluates its methods and performance in relation to handling personal information
10. All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

## 7. DATA TRANSFERS

[Organisation Name] have a Data Transfers Policy and Schedule which lists all the systems, applications or services that may transfer data outside the EU. This also lists the measures taken to ensure that personally identifiable data is private, safe and secure using appropriate technical and organisational measures .

## 8. DATA PROTECTION RIGHTS

We will respect Data Protection Rights. Under the GDPR, individuals will have the right to obtain:

1. confirmation that their data is being processed;
2. access to their personal data; and
3. other supplementary information

a. the purposes of the processing;
b. the categories of personal data concerned;
c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f. the right to lodge a complaint with a supervisory authority;
g. where the personal data are not collected from the data subject, any available information as to their source;
h. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

## 9. DOCUMENT CONTROL

[document owner] is the owner of this document and is responsible for ensuring that this procedure or process is reviewed in line with the review requirements.

Consultation Phase: A document which is circulated for comment to key stakeholders to ensure support for scope, format, and content.

Draft Phase: Ostensibly the last draft, capturing all the points from the previous consultation phase and circulated for comment before being finalised.

Final Phase: A document which is FINAL. This is the baseline document which may subsequently amend over time.

| VERSION | DESCRIPTION OF CHANGE | AUTHOR | APPROVAL | DATE OF ISSUE |
|---|---|---|---|---|
| Consultation | Initial Issue for consultation. | [Author] | [Approver] | March 2018 |
| | | | | |