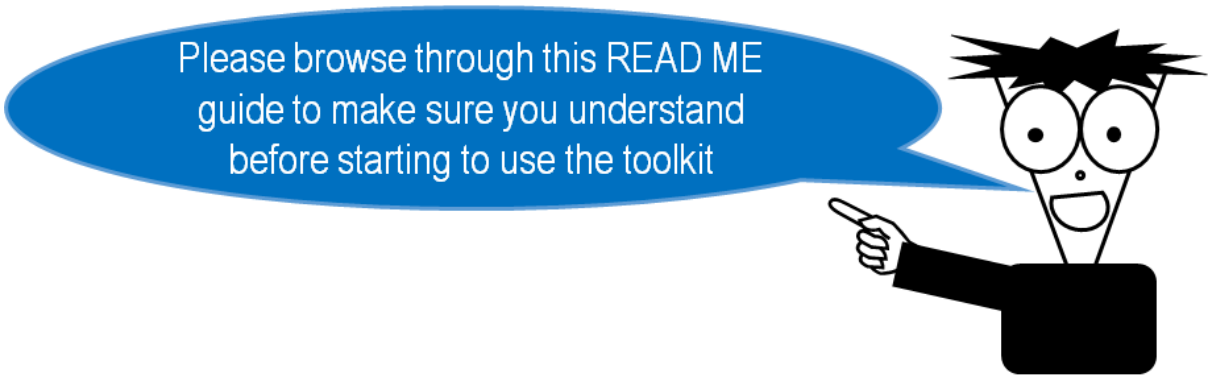
GDPR Toolkit

SUBJECT ACCESS 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

SUBJECT ACCESS REQUEST PROCEDURE

TITLE	ACC GDPR Information security policy.docx	DATE	10/04/18
LOCATION	V:\Data2018\product_gdprtoolkit\ACC GDPR Information security policy.docx	VERSION	Ver 1
AUTHOR	[Author]	Pages	3 of 13
APPROVER	[Approver]		

Contents

1. INTRODUCTION

The purpose of this document is to explain subject access requests, outline a process and propose simple templates for review and approval by [Organisation name].

The work is based on guidance from the UK ICO and existing subject access request process from [Organisation name] (now updated for GDPR) 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. SCOPE

Any request where a member of the public or member of [Organisation name] staff, asks for personal information relating to them to be provided in permanent form should be considered as a subject access request.

Note personal information requests are different from non-personal Freedom of Information Requests which are handled differently

Information is taken to encompass data, information and knowledge assets and is inclusive of all formats whether paper, electronic or media based.

This policy relates to information held by [Organisation name] and any organisation providing services on behalf of [Organisation name](i.e. data processors).

3. GDPR GUIDACE AND SUBJECT ACCESS REQUEST

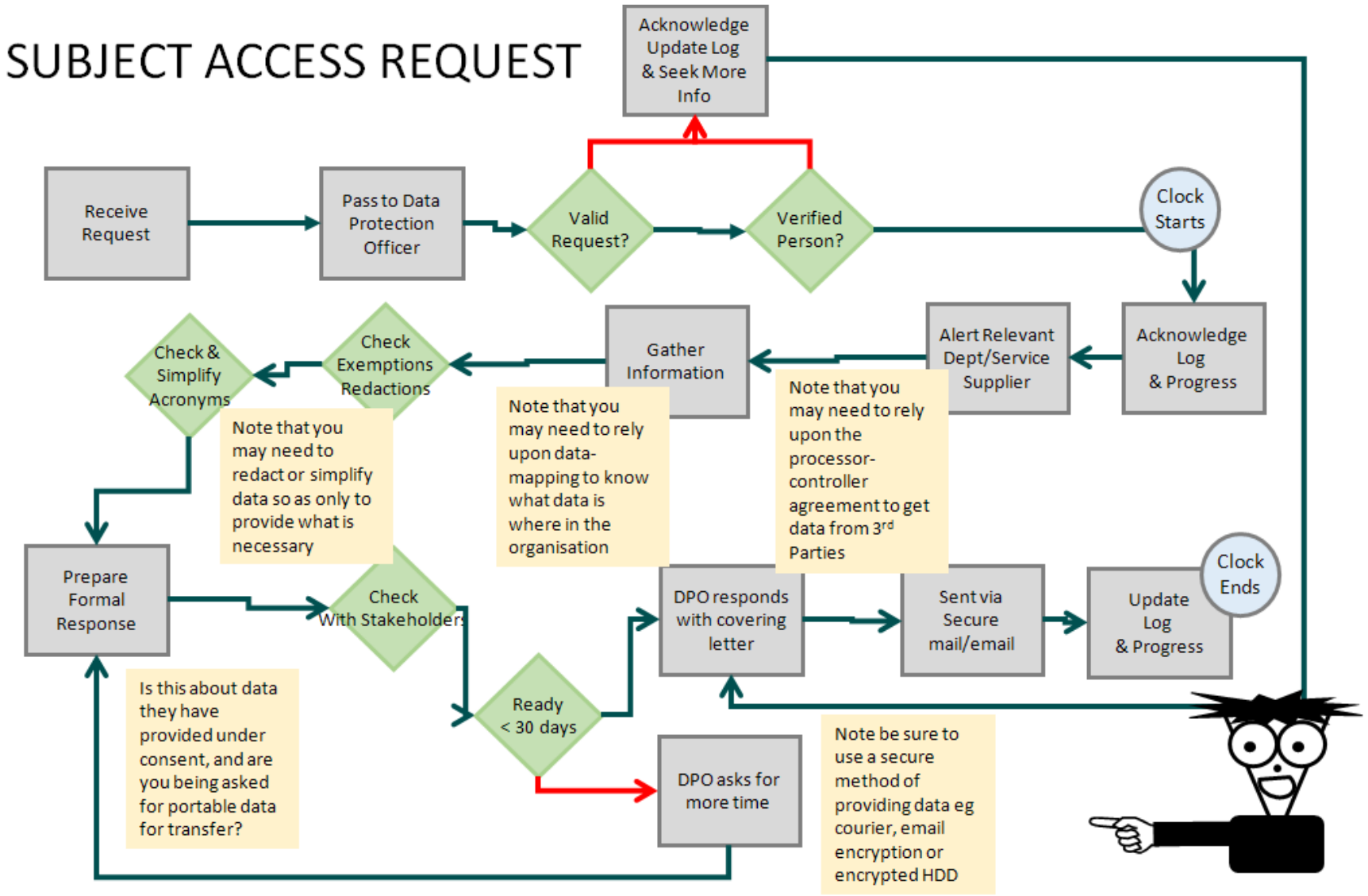
Under the GDPR, individuals will have the right to obtain:

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, referred 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.

4. FACTORS TO CONSIDER WHEN RESPONDING

1. Is it a subject access request?
2. Do you have enough information to be sure of the requester's identity?
3. Do you need more information from the requester to find what they want?
4. Do you have the information the requester wants?
5. Will the information be changed between receiving the request and sending the response?
6. Does it include information about other people?
7. Are you obliged to supply the information?
8. Does the information contain any complex codes or terms?



5. OUTLINE PROCESS

A. Making the Request

For a subject access request to be valid, it should be made in writing. A request sent by email or fax is as valid as one sent in hard copy.

If a request does not mention the Data Protection (Jersey) Law, specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.

A request is valid even if the individual has not sent it directly to the [Data Protection Role] who normally deals with such requests – so it is important that all [Organisation name] staff can recognise a subject access request and treat it appropriately.

If necessary a member of staff should explain to the individual how to make a valid request.

If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may have to make a reasonable adjustment for them. This could include treating a verbal request for information as though it were a valid subject access request, and respond in a particular format which is accessible to the disabled person.

All staff, whether former or current have the right to request access to their personnel file through a subject access request

All requests must be co-ordinated by and responded through the appointed [Data Protection Role].

B. Confirming the Identity

You must confirm the person's identity by what-ever means necessary.

You must not disclose personal data to anyone who does not have a valid legal reason to have that data.

As standard procedure, the [Data Protection Role] will request a copy of:

- Drivers licence, passport or birth certificate as proof of identification.

- A utility bill or [Organisation name] correspondence on headed paper as proof of address.

This information can be sent as a photocopy in the post or as a scanned image.

Requests may be made on behalf of the data subject, such as a solicitor or a family member where they have legal authority (for example by virtue of a court-order). Beware, for example, of giving information to someone who is a former or estranged partner seeking details about someone else.

Requests made on behalf of an individual must contain a letter of signed authorisation from the data subject in addition to the forms of identification.

If the requestor is a current member of staff and the request is sent from a [Organisation name] email address then no additional identification will be required.

C. Logging the Request

GDPR requires that all requests for personal information should be satisfied within 4 weeks ([Organisation name] will aim to respond within 30 calendar days, or 20 working days) .It is therefore vital to log and record progress.

All requests for personal information received should be forwarded to the [Data Protection Role] as soon as they are received, who will log and acknowledge the request

The period of 4 weeks may be extended by a further 8 weeks where necessary, taking into account the complexity and number of the requests, and the controller must inform the data subject of any such extension within 4 weeks of receipt of the request, together with the reasons for the delay.

All requests received in hard-copy format should be date stamped.

D. Acknowledging the Request

All requests for personal information should be acknowledged within 3 working days by the [Data Protection Role].

In some cases, personal data may be difficult to retrieve and collate. If further information is reasonably required to find the personal data covered by the request, or to confirm the identity or authority of the person making the request (see above) then the [Data Protection Role] will request this in writing.

The [Organisation name] need not comply with the subject access request until this information is received.

The right of subject access applies whatever the motive of the data subject for seeking the information. Whilst we are allowed to clarify the request, we are not entitled to ask the data subject why they are seeking the information.

However in many cases the information being requested by available in the data-subject's contract or Privacy Notice, and [Organisation name] may refer the data-subject to this to confirm whether any further information is needed.

Once the above points have been satisfied, the statutory 30 day period for responding begins. At this stage the requestor will be contacted in writing to inform them that we are satisfied with the request and to communicate the deadline date.

E. Requests made on behalf of Children

The Data Protection (Jersey) Law, specifies the age from which children may exercise or enforce their rights as 13. However some 13 year-old are very mature and some are less mature and you should exercise extreme caution in releasing personal data about Children.

Information Commissioner guidance does state that where data subjects are incapable of understanding or exercising their rights, for instance because they are too young, subject access requests can be made by parents or other persons who are legally able to act on behalf of the data subjects (for example, if they have an enduring power of attorney).

A parent or guardian does not have an automatic right of access to their dependant's records.

It is important that the request is made on behalf of the data subject, and not in the interests of the requester. The Data Processing Officer will decide on behalf of the Data Controller as to whether a request will be refused if it is felt that it is not in the best interests of the data subject to release this, and will document their decision.

Where requests are made on behalf of a child, the Data Processing Officer and the service area representative will consider whether the information was provided by the data subject in the expectation that it would not be disclosed to the person making the request, i.e. whether the information is covered by a common law duty of confidence.

F. Repeated or unreasonable requests

The Data Protection (Jersey) Law, does not limit the number of subject access requests an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are vexatious.

Where requests from a data subject are manifestly vexatious, unfounded or excessive, in particular because of their repetitive character, the burden of proving which is on the [Organisation name], the [Organisation name] may either –

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the other action requested; or
(b) refuse to act on the request.

G. Collation of information

All departments that handle personal and/or sensitive information are responsible for supporting the [Data Protection Role] ensuing that requests are responded to promptly and appropriately and within the 4 week period (20 working days).

Requests for information from staff will be co-ordinated by the HR department and [Data Protection Role] who will request information from managers.

Manager should collate the information they hold and provide it to the [Data Protection Role] to send out within 25 calendar days. This will ensure that the [Data Protection Role] is able to compile the information and approve and exemptions or redactions. However, all requests should be dealt with promptly and as a matter of priority.

Clear time scales must be given to third parties, officers and other professionals to respond to enquiries relating to the request.

The requested data must be supplied in intelligible and permanent form, unless this is not possible or would involve disproportionate effort.

Managers should search for the requested data on the relevant databases, computer or email systems, and in their paper filing systems, and print out or photocopy all the requested information. This may be delegated to another officer if appropriate.

They must then:

- CHECK the material for any references to third parties.
- CHECK that any acronyms or codes are explained
- DECIDE whether there are grounds for withholding any information under the exemptions.

Any decisions to withhold information must be confirmed with the [Data Protection Role] and documented on the requesters file.

The [Data Protection Role] will then make the necessary redactions, and will ensure that an original copy is retained on file for audit purposes.

Managers should consider whether it is appropriate to offer the requester support to understand or read the information. This is especially relevant for requests for records which may include sensitive or specialist information.

Once the request (irrespective of whether from individual and / or from third party) has been received, no amendments or deletions must be made to the data that would not have been otherwise made. The data must not be tampered with in order to make it acceptable.

H. Sending the response

All the information, irrespective of the originating department, should normally be sent as one response.

A covering letter should accompany the response and should detail the following:

a. The source of the information released,

b. The organisations purpose in processing this data,

c. If information has been withheld, details of the exemption used,

d. If no information has been found, a statement to that effect,

e. Details of any acronyms, special codes or specialist terms used within a document,

f. The Record Management Officer's contact details in the event of further queries.

If information is posted, it must be sent by special delivery. Alternatively, the [Data Protection Role] will invite the customer/data subject into the office to collect.

If information is emailed, it must be sent in an encrypted format, and users will be asked to contact [Organisation name] for the password. .

I. Complaints

It is a requirement of GDPR that the data-subject's rights (see above) including the right to complain must be notified to the data-subject in their contract or relevant Privacy Notice.

If an individual is unhappy with the process of providing the information, or feels that the information is incomplete, [Organisation name] will initially attempt a local resolution.

The [Data Protection Role] will in the first instance deal with any complaints, and will subsequently liaise with the relevant department manager

If the complaint cannot be resolved satisfactorily, then the [Organisation name] will recommend that the Data Subject contacts the Information Commission Office directly.

J. Internal Assurance

An annual review of systems of internal control over handling requests will be conducted by the [Data Protection Role].

The conclusions of this review will be presented to the Board as part of data-protection governance.

K. Training and awareness

Staff will be made aware of this procedure as part of GDPR Awareness and on a regular basis afterwards through the organisation's internal communications channels.

New staff will be informed of the procedure and GDPR Awareness through the mandatory training as part of the induction process.

Managers are responsible for ensuring that their staff are sufficiently aware of this procedure, and GDPR Awareness in general and any associated guidance to carry out their role.

6. 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