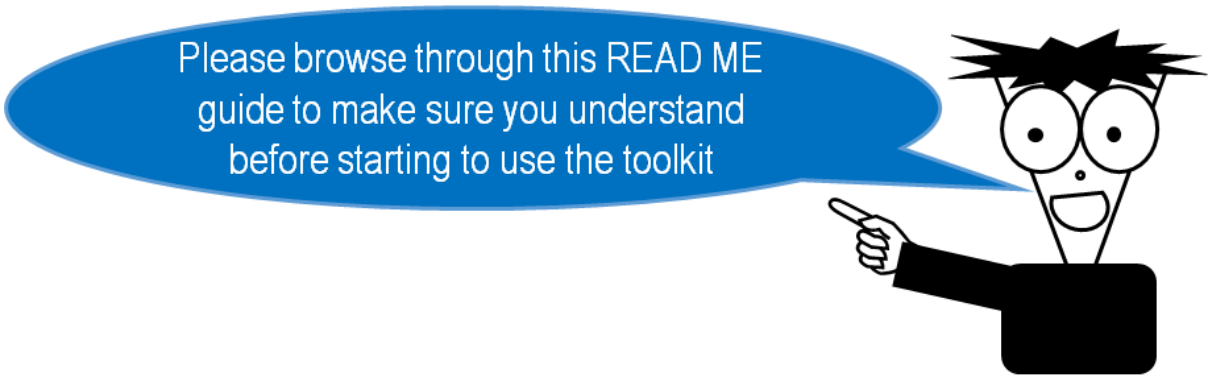
GDPR Toolkit

DATA PROTECTION IMPACT ASSESSMENT

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

TITLE	ACC GDPR Data protection impact assessment procedure.docx	DATE	10/04/18
LOCATION	V:\Data2018\product_gdprtoolkit\ACC GDPR Data protection impact assessment procedure.docx	VERSION	Ver 1
AUTHOR	[Author]	Pages	3 of 10
APPROVER	[Approver]		

1. POLICY GUIDANCE

This policy and procedure 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

You must do a DPIA for certain types of processing, or any other processing that is likely to result in a high risk to individuals. You can use our screening checklists to help you decide when to do a DPIA.

A data processing impact assessment DPIA must…

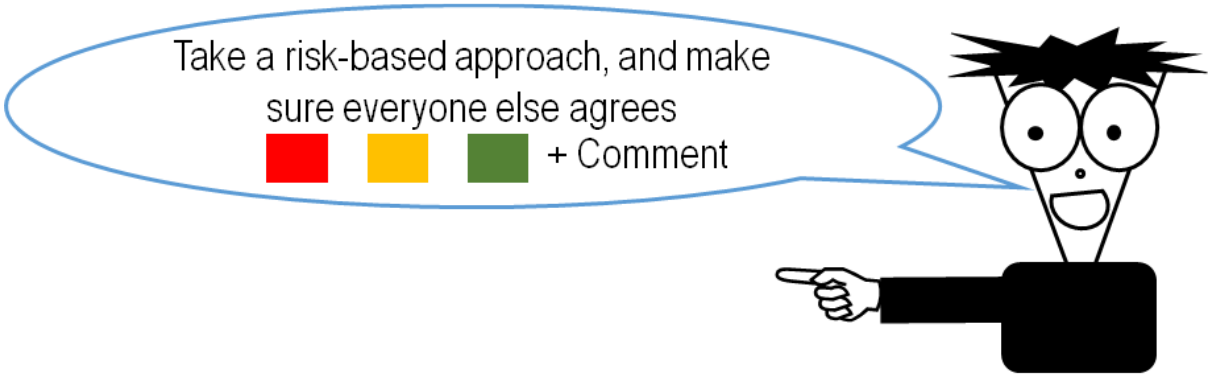
1. describe the nature, scope, context and purposes of the processing;
2. assess necessity, proportionality and compliance measures;
3. identify and assess risks to individuals; and
4. identify any additional measures to mitigate those risks

DPIAs are a tool to help you identify and minimise the data protection risks of projects or changes. They are part of your accountability obligations under the GDPR, and an integral part of the data protection by default and by design approach. An effective DPIA helps you to identify and fix problems at an early stage, demonstrate compliance with your data protection obligations, meet individuals expectations of privacy and help avoid reputational damage which might otherwise occur. In some cases the GDPR says you must carry out a DPIA, but they can be a useful tool in other cases too

DPIAs are an essential part of your accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave you open to enforcement action, including a fine

In particular, the GDPR says you must do a DPIA if you plan to

1. use systematic and extensive profiling with significant effects;
2. process special category or criminal offence data on a large scale;
3. or systematically monitor publicly accessible places on a large scale.

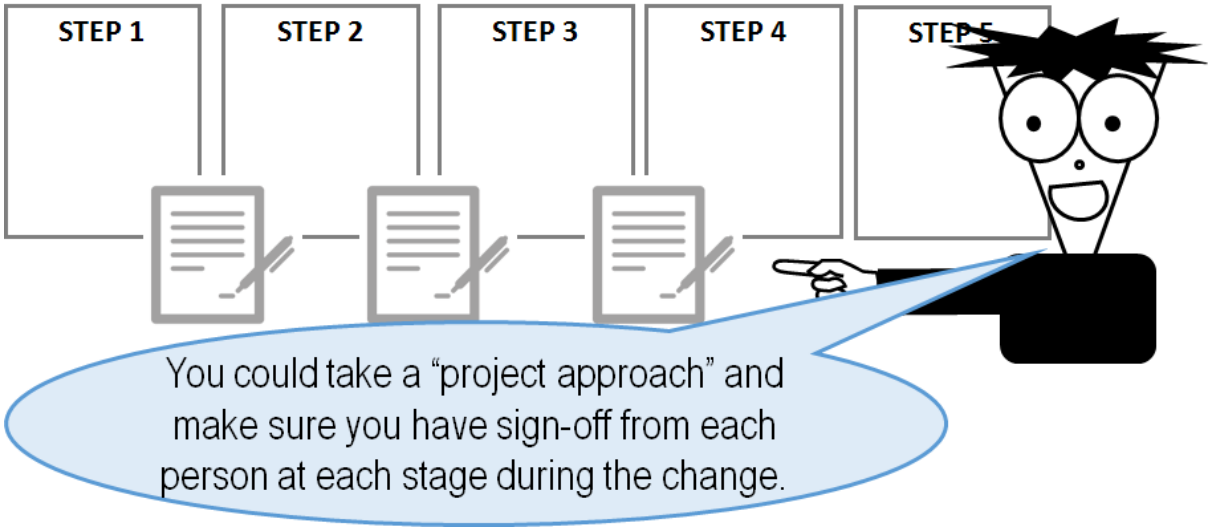


The ICO also requires you to do a DPIA if you plan to:

1. use new technologies;
2. use profiling or special category data to decide on access to services;
3. profile individuals on a large scale;
4. process biometric data;
5. process genetic data;
6. match data or combine datasets from different sources;
7. collect personal data from a source other than the individual without providing them with a privacy notice(invisible processing);
8. track individuals location or behaviour;
9. profile children or target marketing or online services at them;
10. or process data that might endanger the individuals physical health or safety n the event of a security breach

A DPIA also brings broader compliance benefits, as it can bean effective way to assess and demonstrate your compliance with all data protection principles and obligations.

2. PROCEDURE STEPS



Step 1: identify the need for a DPIA
Step 2: describe the processing
Step 3: consider consultation
Step 4: assess necessity and proportionality
Step 5: identify and assess risks
Step 6: identify measures to mitigate the risks
Step 7: sign off and record outcomes
Step 8: integrate outcomes into project plan
Step 9: keep your DPIA under review

If you have a DPO, you must seek their advice. The DPO should provide advice on:

1. whether you need to do a DPIA;
2. how you should do a DPIA;
3. whether to outsource the DPIA or do it in-house;
4. what measures and safeguards you can take to mitigate risks;
5. whether you've done the DPIA correctly;
6. andthe outcome of the DPIA and whether the processing can go ahead.

You should record your DPOs advice on the DPIA.

3. 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

GDPRToolkit

DATA PROTECTION IMPACT ASSESSMENT FORM

Step 1: Identify The Need For A Dpia

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA

Step 2: Describe The Processing

Describe the nature of the processing : how will you collect, use , store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or an other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing : what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing : what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws ? Is it novel in any way? What is the current state of technology in this area? Are there any current issues o f public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing : what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step 3: Consider Consultation

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals views or justify why it s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess Necessity And Proportionality

Describe compliance and proportionality measures , in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify And Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. Consider Risk x Likelihood = Impact and therefore the Actions to reduce risk or minimise impact.

Step 6: Identify Measures To Mitigate The Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk

Step 7: Sign Off And Record Outcomes

Describe the nature of the processing : how will you collect, use , store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or an other way of describing data flows. What types of processing identified as likely high risk are involved?

Step 8: Integrate Outcomes Into Project Plan

Describe the nature of the processing : how will you collect, use , store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or an other way of describing data flows. What types of processing identified as likely high risk are involved?

Step 9: Keep Your Dpia Under Review

Describe the nature of the processing : how will you collect, use , store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or an other way of describing data flows. What types of processing identified as likely high risk are involved?

GDPRToolkit

Sign-Off / Approval

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