GDPR Toolkit

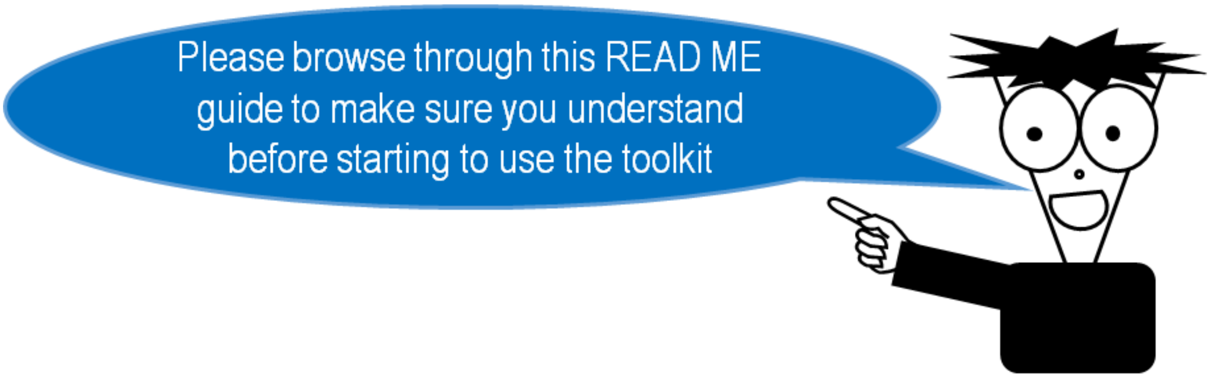
DATA PROCESSOR AGREEMENT

Do not use as-is, but make necessary amendments relevant to your organisation

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.


Please browse through this READ ME guide to make sure you understand before starting to use the toolkit

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

PROCESSOR-CONTROLLER AGREEMENT

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 8
APPROVER	[Approver]		

PROCESSOR-CONTROLLER POLICY

This policy and 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

Key resource: https://gdpr-info.eu/

Art. 24 GDPR Responsibility of the controller
Art. 28 GDPR Processor
Art. 29 GDPR Processing under the authority of the controller
Art. 30 GDPR Records of processing activities
Art. 32 GDPR Security of processing

Controller
If you act as a controller, you must keep a record of the following information:

1. your name and contact details and, where applicable, any joint controllers, representatives and data protection officers;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients, including recipients in third countries or international organisations;
5. details of transfers of personal data to third countries (where applicable);
6. retention periods for different categories of personal data (where possible); and
7. a general description of the security measures employed (where possible).

Processor
If you act as a data processor, you must keep the following records:

1. your name and contact details and, where applicable, representatives and data protection officers;

2. the name and contact details of each controller you act for including, where applicable, representatives and data protection officers
3. the categories of processing carried out on behalf of each controller;
4. details of transfers of personal data to third countries (where applicable);
5. a general description of the security measures employed (where possible).

Additional Guidance
https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

PROCESSOR-CONTROLLER PROCEDURE

In some cases it may be appropriate to have a formal contract (Processor-Controller Agreement) to document the roles, goals, controls and responsibilities as well as any relevant due diligence on the people, process and technology to be used.

In other cases, for example if using services of Google, Microsoft or other suppliers who are not going to enter into a one-to-one relationship there should be nonetheless an objective appraisal and consideration of the controls, checks, monitoring covering people, process and technology to be used.

GDPRToolkit

DUE DILIGENCE TEMPLATE

For some organisations with Cyber Essentials, ISO27001, or SOC2 there may be a very complex questionnaire that can be applied, but the following are simple minimal questions that the vendor should be able to confirm, or you should be able to find out from their website.

People

Describe what role based access controls you have that restrict access to our data and, where relevant, what staff vetting and monitoring do you do to ensure people only access information on a “need to know” basis.

Process

Describe the process controls that you operate to safeguard our data. If it is easier to refer to documents, standards, accreditations etc. please provide these.

Technology

Describe the technology controls that you operate to safeguard our data. The minimum requirement is those that comply with Cyber Essentials

https://www.gov.je/stayingsafe/besafeonline/protectyourbusinessonline/pages/cyberessentials.aspx

Documents

Please provide copies of, or links to, the following

1. Privacy Notice
2. Data Protection Policy
3. Any documents, standards, accreditations relevant to IT or data security

PROCESSOR-CONTROLLER TEMPLATE

CONTOLLER	
CONTROLLR DPO	
PROCESSOR	
PROCESSOR DPO	
CONTRACT SCOPE	
The Service	
The Data	
The Purpose	
The Period	
KEY TERMS	1. the processor must only act on the written instructions of the controller (unless required by law to act without such instructions); 2. the processor must ensure that people processing the data are subject to a duty of confidence; 3. the processor must take appropriate measures to ensure the security of processing; 4. the processor must only engage a sub-processor with the prior consent of the data controller and a written contract; 5. the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR; 6. the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; 7. the processor must delete or return all personal data to the controller as requested at the end of the contract; and 8. the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
OTHER TERMS	
SECURITY MEASURES	
SUB -PROCESSORS	
LIABILITIES	
WARRANTIES	

GDPRToolkit

1. 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

FORM

DEPARTMENT	
MANAGER	
DATE	

CONTOLLER	
CONTROLLR DPO	
PROCESSOR	
PROCESSOR DPO	
CONTRACT SCOPE	
The Service	
The Data	
The Purpose	
The Period	
KEY TERMS	1. the processor must only act on the written instructions of the controller (unless required by law to act without such instructions); 2. the processor must ensure that people processing the data are subject to a duty of confidence; 3. the processor must take appropriate measures to ensure the security of processing; 4. the processor must only engage a sub-processor with the prior consent of the data controller and a written contract; 5. the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR; 6. the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; 7. the processor must delete or return all personal data to the controller as requested at the end of the contract; and 8. the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
OTHER TERMS	
SECURITY MEASURES	
SUB -PROCESSORS	
LIABILITIES	
WARRANTIES	

Sign-Off / Approval

Do not use as-is, but make necessary amendments relevant to your organisation