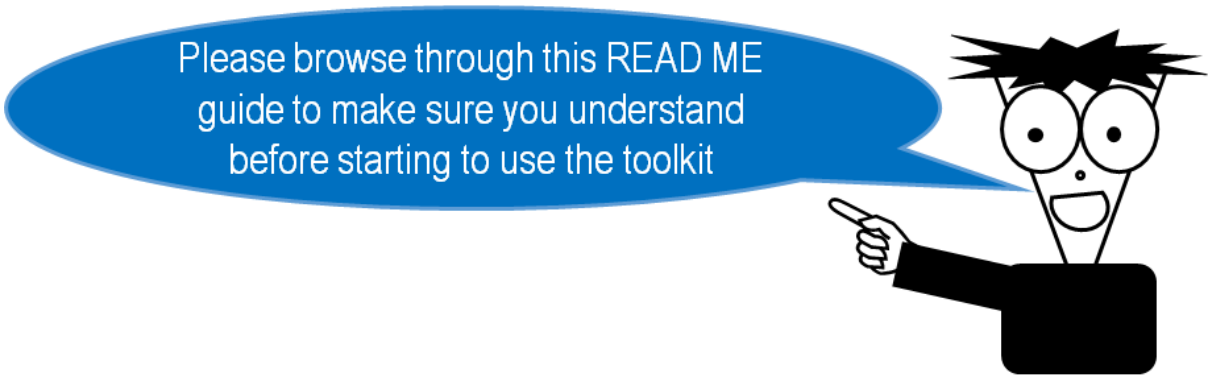
GDPR Toolkit

BREACH POLICY & PROCEDURE

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

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. DATA PROCESSING BREACH MANAGEMENT

Inevitably there may be some data-processing and personal data implications to any security incident, either minor or major.

Therefore the DPO and personal data considerations are a component of both Incident Management and Major Incident Management, as well as Disaster Recovery and Business Continuity Planning.

This should apply to the [Organisation name]and any supplier who hold or process personal data (necessarily under a data-processor agreement)

3. DATA BREACH GUIDANCE

Being Prepared

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

Notifying The Information Commission Officer

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Failing to notify a breach when required to do so can result in a fine. The fine can be combined the ICO's other corrective powers

Notifying The Data Subjects

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

1. the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
2. a description of the likely consequences of the personal data breach; and
3. a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

You do not need to notify the Data Subjects if

1. There are proportionate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular measures that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

2. subsequent measures have been taken which ensure that the high risk to the rights and freedoms of data subjects are no longer likely to materialize; or
3. it would involve disproportionate effort, in which case there must instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Key references
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

See the advice given by Carey Olsen in relation to Data Controller/Processor Agreements, which also mention Breach Procedures (because 3rd parties need to comply with the Breach Procedures agreed in the Controller/Processor Agreements)

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

4. DATA BREACH PROCEDURES

The procedure outlined below is designed to satisfy the requirements of the ICO

1. Know how to recognise a personal data breach.(a personal data breach isn't only about loss or theft of personal data.)
2. Staff knowledge how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
3. Supplier knowledge how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
4. Allocated responsibility for managing breaches to a dedicated person or team.
5. A prepared a response plan for addressing any personal data breaches that occur.

Recognising A Personal Data Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the Data Or Passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Staff Knowledge How To Escalate A Security Incident

All staff are aware of How To Escalate A Security Incident by virtue of regular training and GDPR Awareness.

Supplier Knowledge How To Escalate A Security Incident

All supplier are aware of How To Escalate A Security Incident by virtue of the data controller-processor agreement that exists between [Organisation name] and the suppler and which sets-out the responsibilities of each party.

Responsibility For Managing Breaches

All aspects of Breaches to be managed, controlled and co-ordinated by the Data Protection Officer(s)

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

Example: The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

Within [Organisation name] the Data Protection Officer may have regard to the data-processing-impact assessments and data classification when considering the risk and impact and need to notify ICO.

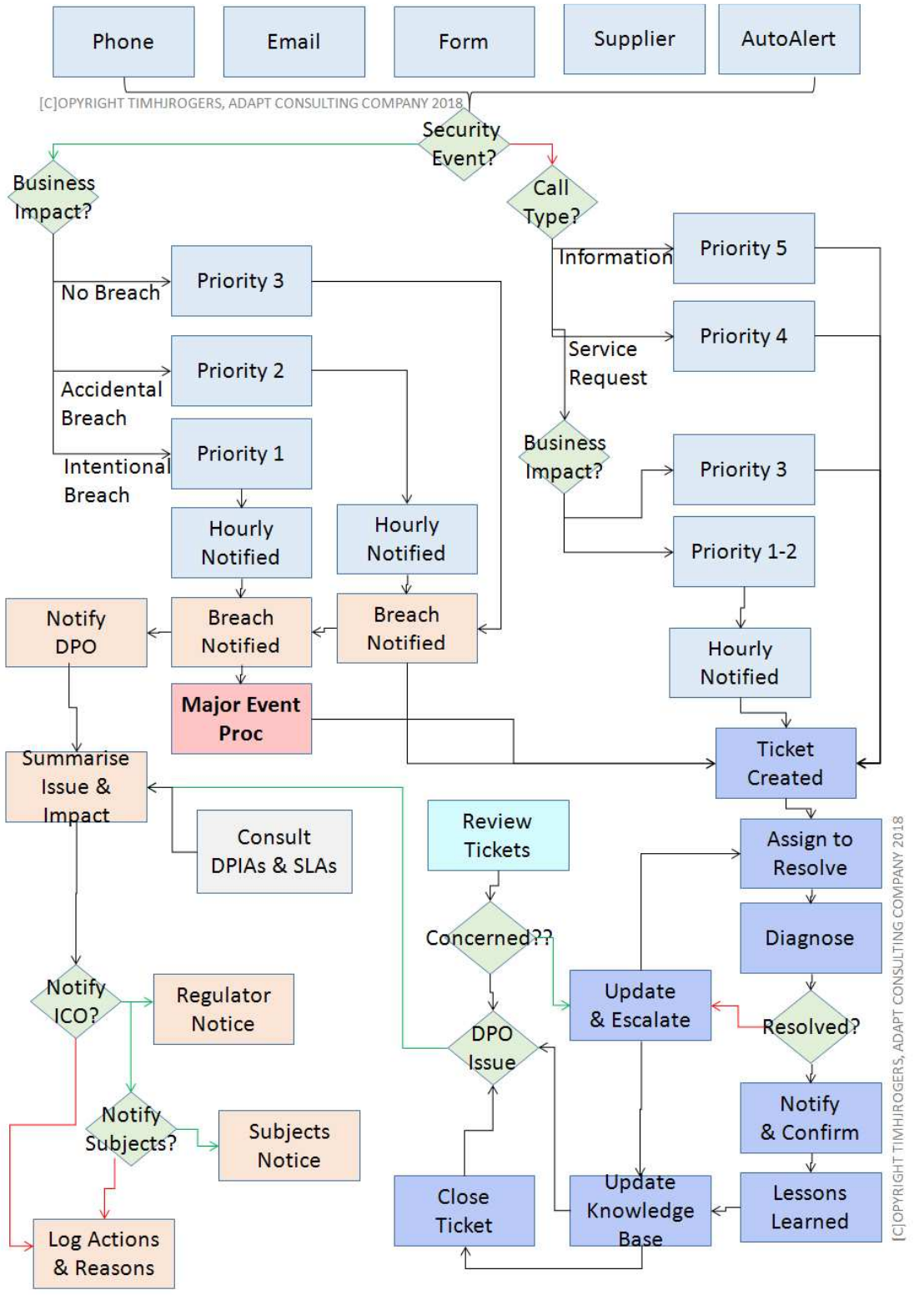
Note the data-processing-impact assessments and data classification are in other documents.

A Response Plan

Inevitably there may be some data-processing and personal data implications to any security incident, either minor or major.

Therefore the DPO and personal data considerations are a component of both Incident Management and Major Incident Management, as well as Disaster Recovery and Business Continuity Planning.

GDPRToolkit



Key reference
https://ico.org.uk/for-organisations/report-a-breach/

5. DATA BREACH TEMPLATE FOR RESPONSES

Template for Notifying ICO

Dear {Regulator}

Urgent Message re Breach Notification

It has been brought to our attention that some personally identifiable data may have been compromised in a security incident. We are writing to alert you to this and explain the implications and actions that we taking.

What data is affected

The following data may be affected {1} Bank-Account; {2} home-address; {3} home-email; {4} home-phone; {5} IT IS-Tax; {6} JY-SocSec; {7} mobile-phone; {8} name; {9} work-address; {10} work-email; {11} work-phone; {12} car-registration {13} boat-registration {14} plane-registration {15} staff-medical-information; {16} staff-health&safetyinformation

Who is affected

The following data-subjects may be impacted by this

Boat Owners (126)
Airport Passengers (7,678,999)
Car Park Users (678,999)

We use a data-classification system to manage risk and identify the necessary controls to apply (attached) and this data is classified as….{add details here to indicate the implications/magnitude of the problem}

Potential Impact

As part of our Data Protection Policy we have done a Data-Processing Impact Assessment, a copy of which is attached.

DPO and Investigation Team

We take information security seriously and we have launched an immediate investigation which is on-going. We will announce updated on-line on our website here: www.ports.je/breachnotifiation

Our Data Processing Officer is Claire Brown Telephone 123456789

What actions that we are taking

We take information security seriously and we have launched an immediate investigation which is on-going. We will announce updates on-line on our website here: www.ports.je/breachnotifiation

We have a prepared an announcement to all affected Data Subjects which will be sent/published {explain: email? Website? Twitter? Facebook?}

We will provide details of the issue together with copies of supporting policies and agreements, plus details of the outcome and lessons learned from the internal investigation, as soon as we are able.

Note not all data/text will be relevant in all cases, the above is just a guide only

Template for Notifying Data Subjects

Dear {Customer Name}

Urgent Message re Information Security

It has been brought to our attention that your data may have been compromised in a security incident. We are writing to alert you to this and explain the implications and actions that we recommend that you take immediately.

What data is affected

The following data may be affected

What actions that we are taking

We take information security seriously and we have launched an immediate investigation which is on-going. We will announce updated on-line on our website here: www.ports.je/breachnotifiation

What actions that we recommend that you take immediately.

Pending the outcome of our investigation and further guidance we recommend that you immediately

- Change your password for all systems that use this password
- Check alert your bank and check your account

- Check alert your credit card provider and check your account

How to find out more

We will announce updated on-line on our website here:
www.ports.je/breachnotifiation

You can also contact our Data Processing Officer, Claire Brown Telephone 123456789

Note not all data/text will be relevant in all cases, the above is just a guide only

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

.