GDPR Handbook and Toolkit

A comprehensive guide and toolkit for delivering the General Data Protection Regulation

Version 0.1, draft
Published xxx 2018

Business Morphology

Business Morphology Ltd. Registered in England No. 5601319
Registered Office: Northside House, Mount Pleasant, Barnet, Herts. EN4 9EE

Table of Contents

1. About this Handbook

About this Handbook

This handbook has been produced by Business Morphology Ltd, whose consultants have become Subject Matter Experts in the General Data Protection Regulation (GDPR). They have already implemented the GDPR for micro and small businesses.

This handbook aims to provide practical advice and guidance to help micro and small organisations navigate their way through the GDPR to achieve compliance. It includes a guide to qualifying what is relevant to a particular organisation, presentations, practical examples, templates, instructions on how to complete each template and extracts of completed templates. For ease of reference to guidance from the UK's data protection regulatory body, the Information Commissioner's Office (ICO), terminology in this handbook is aligned with guidance produced by the ICO, as permitted under the terms of the ICO's Open Government Licence.

To gain an overall understanding of the contents users should first read the whole handbook, and then work through it in the order in which it is written.

Each section follows a similar format throughout, with an introduction at the start of each section. Hyperlinks are embedded to help users navigate quickly to related sections. Various types of content are included, to illustrate what to do, and to provide the tools necessary for an organisation to implement the GDPR themselves. In addition to general guidance and explanations, the following are used throughout the handbook:

- Template – this is a document that contains relevant headings and is ready for an organisation to enter their own text. Where square brackets are used, these should be replaced with an organisation's specific details, eg. [Organisation] might be replaced with AnyOrg Ltd, and [address] might be replaced with 123 The Street, Anytown, Surrey AB1 2YZ
- Extract – this is a section from a completed template, to show what the template looks like when it is populated
- Example – this is NOT a template: it is an example to show what a completed document might look like (eg. a Privacy Statement) and should not be assumed as perfect for any particular organisation. Text may be cut, pasted and edited to suit an organisation, and supplemented as required. A fictitious company, AnyOrg Ltd, is used in the examples

Use of the handbook and templates assumes a basic level of understanding of the Microsoft Office Suite, particularly MS Excel, to enable population of cells, use of filters and search facilities. All content of this handbook is basic standard functionality, for which help is readily available from Microsoft's help pages.

To provide a record of an organisation's GDPR compliance activities, and to provide a reference document for future use, it is recommended that the user copies this handbook, removes all examples, and populates it with specific content relevant to the user's own organisation.

This handbook does not include templates or examples for documents that are not part of GDPR. Users should identify and modify their organisation's documents as required (paper and digital), paying attention to, for example, anything that includes customer-facing communication, training, policies, procedures and 3rd party contracts.

Disclaimer

This handbook is provided on the understanding that is does not constitute legal advice. Use of, and reliance on, this handbook and the contents thereof, is at the user's sole risk. Examples and templates are intended to be used as a starting point from which an organisation can create their own documents and to which all reasonable quality checks should be applied by the user before use. Business Morphology Ltd makes no claims about the accuracy, adequacy or completeness of the contents of this handbook, assumes no duty of care with respect to the contents, and expressly excludes and disclaims liability for any cost, expense, loss or damage suffered or incurred as a consequence of a user's reliance on the contents herein. It is the user's responsibility to ensure that the scope and contents of any document they create is complete, correct and appropriate for their needs. Business Morphology Ltd does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that organisations are in compliance with any law or regulation of England and Wales, under which jurisdiction this Handbook is effected. The user should take reasonable and proper legal and/or other professional advice.

2. Scope and Impact of the GDPR

3.1. General Summary of the GDPR

General Summary of the GDPR - for information	
Effective date	• The General Data Protection Regulation (GDPR) was published on 4 May 2016 to replace the Data Protection Act 1998: enforcement begins **25 May 2018** • The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR
Aims and objectives	• EU data protection law aims to govern the processing of personal data and to ensure that such processing is fair and lawful. It is also designed to give effect to the fundamental right to privacy and to give data subjects greater control over use and retention of their data. • A harmonised approach under the GDPR should increase organisations' ability to transact activities across the EU, with fewer inconsistent national compliance requirements, thereby providing greater legal certainty for organisations. • Anyone who processes personal information must still comply with eight principles of the <u>current</u> Data Protection Act, which make sure that personal information is: 1) fairly and lawfully processed; 2) processed for limited purposes; 3) adequate, relevant and not excessive; 4) accurate and up to date; 5) not kept for longer than is necessary; 6) processed in line with your rights; 7) secure; and 8) not transferred to other countries without adequate protection. • These principles in the law are fit for purpose and are technology-neutral.
What is in scope	• It applies to the processing (ie collection, retention and transfer) of personal data of natural persons, by automated and non-automated means which form part of a filing system or are intended to form part of a filing system. • It applies across all sectors, to all organisations subject to the law.
What is out of scope	It does not apply to: • people who are processing personal data in the course of their own exclusively personal or household activity; • activities that fall outside the scope of Union law, Member state Law or UK Law; or • competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats, to public security.
How it applies to micro organisations and SMEs (which are organisations with fewer than 250 employees)	• The GDPR broadly expects SMEs to comply in full with the Regulation. • SMEs are expected to manage their data flows and data processes to the same extent as larger better-resourced organisations. • They don't need to appoint a data protection officer (DPO) unless **core* activities consist of or involve: ○ systematic monitoring of data subjects on a ***large* scale; or ○ processing on a large scale special categories of data; or ○ personal data relating to convictions and offences. • An SME is exempt from the requirement to maintain a record of processing activities under its responsibility unless the processing: ○ it carries out is likely to result in a risk to the rights and freedoms of data subjects; or ○ is not occasional; or ○ includes special categories of data; or ○ includes personal data relating to criminal convictions and offences. **core* and ***large* have not been defined officially

3.2 What’s Changed

What’s Changed - for information
Definition of Personal data • This is any information: o relating to an identified or identifiable natural person (eg. name, address, telephone number, passport, driving licence reference number, eg. NHS number, NI number, tax reference); o extended to include online identifiers, eg. IP addresses and cookies (if they are capable of being linked back to the data subject); o indirect information, eg. physical, physiological, genetic, mental, economic, cultural or social identities that can be traced back to a specific individual
Privacy by Design • Companies must implement appropriate technical and organisational measures in relation to the nature, scope, context and purposes of their handling and processing of personal data, with data protection safeguards designed into products and services from the earliest stages of development. These safeguards must be appropriate to the degree of risk associated with the data held and might include: o Pseudonymisation and/or encryption of personal data; o Ensuring the ongoing confidentiality, integrity, availability and resilience of systems; o Restoring availability and access to data in a timely manner following a physical or technical incident; and o Introducing a process for regularly testing, assessing, and evaluating the effectiveness of these systems
Territorial Application • Organisations outside the EU will be subject to the GDPR when collecting data concerning any EU citizen
Consent • Consent must be given by the individual whose data is held • Organisations will need to be able to show how and when consent was obtained o Data obtained must be for specific, explicit and legitimate purposes o Data must be erased when no longer needed • Individuals must be able to withdraw consent at any time and have a right to be forgotten if that data is no longer required for the reasons for which it was collected • The lawful basis, or lawful bases, for processing must be made clear
Rights of Data Subjects • Some rights of data subjects are strengthened by the GDPR (eg, the right to object) and some new rights are created (eg, the right to data portability)
72 hours data Breach Notification • Organisations must report data breaches to the relevant Supervisory Authority (SO) within 72 hours of detection o in the UK the SO is the Information Commissioner’s Office, the ICO
Increased compliance obligations for Controllers • New and increased compliance obligations on controllers, eg. o implementing appropriate policies, keeping records of processing activities, privacy by design and by default
Direct compliance obligations for Processors • Processors will have direct legal compliance obligations: DPAs can take enforcement action against processors
Appointing a DPO • Organisations that regularly and systematically monitor data subjects, or process Sensitive Personal Data on a large scale, must appoint a Data Protection Officer ("DPO"): this can be an external person/body
Remedies and Sanctions • For non-compliance: up to €10m or 2% of global gross turnover for violations of record-keeping, security, breach notification, and privacy impact assessment obligations. • Doubled to €20m or 4% of turnover, for violations related to legal justification for processing, lack of consent, data subject rights and cross-border data transfers.
Relationships with other laws • Uncertainty remains regarding the relationship between the GDPR and other laws (e.g., the ePrivacy Directive)

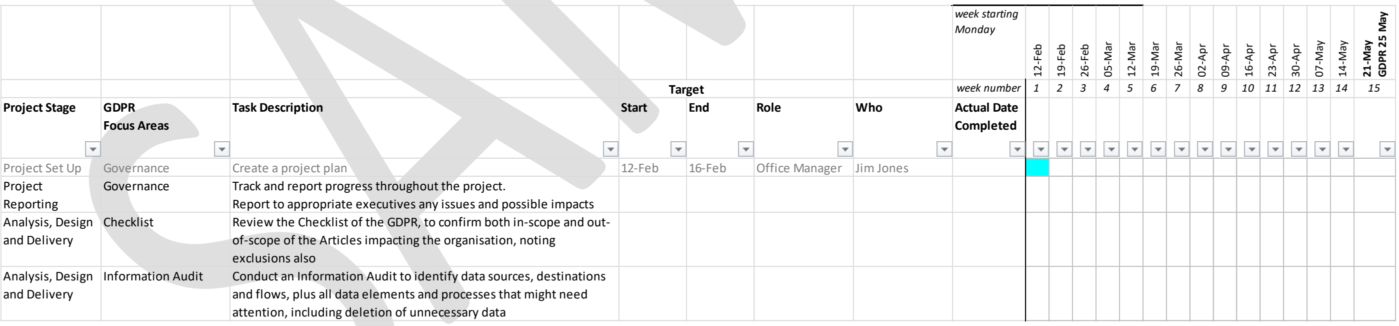
4. Implementation

4.1 GDPR Project Plan, key steps

GDPR Project Plan, key steps	
Project Set Up	• Create a Project Plan. • Agree project roles and who will take the roles. Give start and end dates to each task. • Track and report progress. Report to appropriate executives any issues and possible impacts
Analysis, Design and Delivery	• Review the Checklist of the GDPR, to confirm both in-scope and out-of-scope of the Articles impacting the organisation, noting exclusions also
	• Decide how to approach Organisation Awareness (ie. who needs to know what and when do they need to know it). • Create appropriate internal communications and training plans
	• Conduct an Information Audit to identify data sources, destinations and flows, plus all data elements and processes that might need attention. • If Children are potential audiences ensure this is identified in relevant processes. • Document a list of actions for all areas needing attention, identify the options, agree solutions. • Include deletion of unnecessary data. • If 3rd party systems need remediation, work with the 3rd parties to identify what to do and how to test the changes.
	• Decide how to manage Business Awareness of the GDPR within the organisation (ie. who in the organisation needs to know what and when do they need to know it). • Create appropriate communications and training
	• Review how privacy information is communicated. • If Children are potential audiences ensure the extra protections afforded to them are applied. • Review current Privacy Notices and update as necessary – see Lawful Basis also. • Publish the new Privacy Notices (also known as Privacy Statements) • If necessary advise staff/customers of the new statement and ask for consent if appropriate.
	• Review the set of 08 Individuals' Rights and how these are managed. • If Children are potential audiences ensure the extra protections afforded to them are applied. • Make any changes to processes to manage these Rights and maintaining records thereof
	• Review and update the process for managing Subject Access Requests (SARs) • Modify, as appropriate, the template letters provided for responding to SARs
	• Identify the Lawful Basis, or Bases, under which data is being processed, revise as necessary. • If Children are potential audiences take extra care to ensure the basis/bases is/are appropriate. • Maintain records of the Basis/Bases. • Review and update Privacy Notices to reflect Basis/Bases.
	• If Consent is used as a Lawful Basis ensure it's appropriate and meets all conditions of Consent. • If Children are potential audiences ensure the extra protections afforded to them are applied. • Amend Consent statements and re apply for Consent if necessary. • Update processes to manage Consent.
	• Create a Breach Management system, including Breach Alerting System and Reports, following the process provided for responding to a breach. • Modify, as appropriate, the template letters provided for responding to a breach
	• Review key organisation processes under Data Protection by Design to determine necessity for Data Protection Impact Assessment. • If conditions require a DPIA, use the DPIA template provided
	• Review roles and responsibilities of Data Protection Officers. • Create Job Descriptions (Data Controller and Data Processors examples provided). • Appoint delegates to roles. • Embed these in employees' and 3rd parties' contracts

	• From the Information Audit identify relevance of International transfers: include digital data backup • Confirm if conditions of transfer are met: address exceptions
	• Identify and assess Organisation Risks, define reduction and mitigation measures
	• Create an Activity Log to maintain and evidence records of processing activities and security measures (for production to the ICO if requested)
	• Contact all 3rd Parties about their GDPR compliance. • Track and manage responses.
	• Create/revise other internal processes and documents as necessary, including: application forms; customer/staff documents; manuals; policies and procedures; 3rd party contracts and correspondence; tracking tools.
	• Following the GDPR changes implemented, validate that compliance with non-GDPR regulations is still maintained across all the organisation's processes.
Ongoing and Future Activities	• Start using newly created or updated documents when appropriate to the organisation (eg current stock exhausted), or on 25 May 2017, whichever comes first.
	• Maintain adherence to updated documents, processes, tools, etc.
	• Maintain the Organisation Risk log.
	• Maintain the Definitions Log.
	• Follow schedule to review and update the Activities Log, for production to the ICO if requested.
	• Conduct a DPIA if the organisation considers introducing any new high-risk activities.
	• In case of Breach, follow the Breach Alerting System.

4.2 Project Plan: Extract



							week starting Monday	12-Feb	19-Feb	26-Feb	05-Mar	12-Mar	19-Mar	26-Mar	02-Apr	09-Apr	16-Apr	23-Apr	30-Apr	07-May	14-May	**21-May GDPR 25 May**
			Target				*week number*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Project Stage	**GDPR Focus Areas**	**Task Description**	**Start**	**End**	**Role**	**Who**	**Actual Date Completed**															
Project Set Up	Governance	Create a project plan	12-Feb	16-Feb	Office Manager	Jim Jones		🟦														
Project Reporting	Governance	Track and report progress throughout the project. Report to appropriate executives any issues and possible impacts																				
Analysis, Design and Delivery	Checklist	Review the Checklist of the GDPR, to confirm both in-scope and out-of-scope of the Articles impacting the organisation, noting exclusions also																				
Analysis, Design and Delivery	Information Audit	Conduct an Information Audit to identify data sources, destinations and flows, plus all data elements and processes that might need attention, including deletion of unnecessary data																				

4.3 Project Plan: Template

GDPR Project Plan Template v2.0 18020

6. Business Awareness

6.1 ICO 12 Steps Guidance: Step 1

ICO 12 Steps Guidance - Step 1, Awareness

"You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute."

6.2 Awareness Objectives

Communications Objectives

- To provide an understanding of the key drivers for change and how they link into the broader vision for your organisation;
- To provide a clear understanding of the changes brought by the GDPR and how these will both benefit and impact the organisation and people within it;
- To engage, involve and obtain feedback from impacted stakeholders (ie anyone who has a stake in knowing what's happening) to enable effective working in the future regulatory environment;
- To support the organisation changes with a comprehensive 2-way communications programme and thus facilitate a smooth migration to the future state and beyond; and
- To provide the necessary advice and instruction to help stakeholders prepare for the transition and support them through the changes.

6.3 Who needs to know what

Who needs to know what

Build Awareness with people and groups who require a general level of communication. They are not directly involved in or impacted by changes, but would benefit from knowing what is going on. Typically, this includes general employee audiences, identifiable groups and organisations both internal and external to the organisation

Keep Informed those people who are directly involved in, or impacted by, the changes. Typical examples include users of a new system or process, who will need to know how things are progressing, and how their roles may change, but cannot influence the nature of those changes besides providing feedback

Keep Satisfied any group or people who have a high level of power or influence over the progress of the programme, but are not necessarily directly involved in or impacted by it, but they could be. They are important influencers of the key players, and will often provide the information upon which decisions are made (though they do not themselves directly make the decision). They can be useful advocates, or potentially harmful rumourmongers. If 'change champions' (often existing team leaders) are engaged they can be allies if there is resistance to change

Work Closely with those who have a high level of involvement and a high level of power – these are your key players. They are the individuals with the ability / authority to say 'yes' or 'no' to the changes and the way in which they are implemented

6.4 What to do

What to do

- Tell staff about GDPR in the general sense;
- After working out what changes need to be made:
  - tell specific staff about their roles and responsibilities;
  - contact every organisation with whom personal data is shared – see 3rd Parties Compliance in this handbook;
  - at a level appropriate to their involvement, keep all parties informed of progress of the organisation's GDPR project
  - provide staff with:
    - answers to their questions;
    - a resource (eg a person in the organisation, intranet, specific weblink) to find out more information; and
    - updates about project progress, what will happen next and the longer term plan; and
- Maintain a record of all questions raised and what responses were given

6.5 Awareness Communications: How to Use

How to use the Example Awareness Communications

The examples attached below are designed to give a wide audience their first introduction to the GDPR

1. Edit the documents as required, eg.
   - add/delete content as desired;
   - align with any organisation standards, such as colours and fonts;
   - give a corporate look and feel through the use of corporate logos; and
   - use language appropriate to the audience
2. Keep a record of all questions raised;
   - Commit to providing staff with answers to their questions

Example 1 is a presentation for delivery to staff, eg at a staff meeting

Example 2 is a document that can be read to staff and/or used as a handout

6.6 Awareness Communication: Example 1

In slide show format and PDF

GDPR Presentation Generic Staff v0.1 18

GDPR Presentation Generic Staff v0.1 18

6.7 Awareness Communication: Example 2

In Handout format

GDPR Presentation Generic Staff Handou

APPENDICES

A. Definitions

Glossary of GDPR terms used, or referred to, in this document

GDPR Definitions Log
v1.0 180206.xls

B. Information Security and Governance Policy

Information Security
and Governance Polic

C. GDPR Support

Business Morphology - GDPR Support

Online Help

FAQs and an **email helpline** are available at www.BusinessMorphology.biz. These are private resources, intended only for those who already have this handbook. Passwords will be confirmed with purchase of the handbook.

Workshops, In-house Presentations and Consultancy

- Workshops give a walk-through of the handbook and an opportunity for delegates to ask questions live
- In-house presentations are for organisations that would like a presentation tailored to their requirements
- Consultancy provides tactical support to solve business problems and exploit business opportunities

To find out more about our support and other products please visit www.BusinessMorphology.biz

ICO - GDPR Help, Advice and Funding

Online Help

The Information Commissioner's Office (ICO) provides extensive guidance on the GDPR via their website, Guide to the General Data Protection Regulation (GDPR). There are resources on the ICO website specifically aimed at helping small organisations (those employing fewer than 250 people) to prepare for the GDPR.

Telephone Helpline

The ICO runs a help line dedicated to small businesses, to help them prepare for the new data protection law. The phone service is aimed at people running small businesses or charities and recognises the particular problems they face preparing for the new Regulation. It provides additional, personal advice to small organisations that still have questions. As well as advice on preparing for the GDPR, callers can also ask questions about current data protection rules and other legislation regulated by the ICO including electronic marketing and Freedom of Information.

The ICO Helpline number is 0303 123 1113 - select option 4 to be diverted to staff who can give support. It is available Monday to Friday from 09:00-17:00, except Wednesdays when it closes at 13:00.

ICO Funding post GDPR

Under the 2018 Regulations, data controllers must pay the ICO a data protection fee, unless they are exempt. The ICO has produced a guide explaining the fee structure, costs and exemptions.

The new fee structure is a three tier system, which differentiates according to turnover and number of staff:

- Tier 1, £40: micro organisations, maximum turnover £632,000 per financial year or maximum 10 staff.
- Tier 2, £60: small/med organisations, maximum turnover £36million per financial year or maximum 250 staff.
- Tier 3, £2,900: all other organisations. Note, unless the ICO is informed otherwise it will assume Tier 3 applies.

These fees fund the ICO's data protection work, which includes both the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA).

Attribution to the ICO

Throughout this document there are references to, and extracts from, guidance published on the ICO's GDPR website, to which updates are frequently applied. Use of such material in this Handbook is licensed under the Open Government Licence. The ICO's 12 Steps used in this document were published in a PDF, V2.0 20170525.