Acumenology

business support

ESSENTIAL GDPR COMPLIANCE

A step by step guide
to help small businesses
manage their GDPR compliance

An Acumenology Business Guide

Acumenology.co.uk

Contents

01
Introduction

GDPR compliance is not a tick box exercise but a journey that involves a change in the culture and the manner in which a business manages personal data.

Undertaking compliance will prove challenging, and the time required will depend on the size, complexity and amount of data your business processes.

The Information Commissioners Office (ICO) suggests that the measures an organisation takes should be "risk-based and proportionate" to the size and complexity of the personal data being processed.
Thus, if you have a small business with a few employees and process a relatively limited amount of personal data, the Essential Compliance Roadmap will help you focus on key activities required by the ICO.

However, we recommend that depending on the size, amount of personal data you process, and the nature of your organisation, you customise your compliance activity to suit the level of risk you consider acceptable for your organisation.

In this increasingly litigious world, we strongly recommend a safe low risk approach and suggest you consider compliance in two phases.

Phase 1 – Carry out as a matter of urgency activities set out in the Essential GDPR Compliance Roadmap.
Phase 2 – Choose and carry out other relevant activities at a pace that suit your organisation.

We recognise that you are likely to be extremely busy and that not only does compliance seem complicated but, that it places an increased burden on your time.
The Essential Compliance Roadmap simplifies what is required and provides a 'priority list' of activities regarded as mandatory under the GDPR.

We have provided you an overview on each activity, and there is a lot of information freely available that will assist you in your task.

To further help you, Acumenology has produced a series of Business Guides on a range of relevant topics.
You can find these at: www.acumenology.co.uk/business-guides

02

Essential GDPR Compliance Roadmap

UNDERSTAND
Create awareness develop a plan & provide training

Step 1:
Activity Log
Record all GDPR related activity & keep updated

Step 2:
Staff Training
Provide GDPR awareness training for all staff

DISCOVER
Map data and identify risks

Step 3:
Lawful Basis for Processing
Determine & record your lawful basis for processing

Step 4:
Processor Management
Review contracts with processors and data storage arrangements

IMPLEMENT
Design & implement operational controls

Step 5:
Data Processing Inventory
Recording processing activities

Step 6:
Operational Protocols
Establish data minimisation, retention, disposal & email protocols

Step 7:
Privacy Information
Ensure all notices and privacy policies are compliant

Step 8:
Subject Access Request
Ensure SAR's processes are in place

Step 9:
Data Breach
Ensure Data Breaches protocols & response plans are in place

CONTROL
Manage and enhance controls

Step 10:
Privacy by Design
Ensure Privacy by Design is built in including PIA's as required

MAINTAIN
Ensure on - going compliance

Annual compliance audit

New staff training & on-going training

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

03

Step-by-step guide to GDPR compliance

If you are small business with a few employees, process a relatively limited amount of personal data, the Essential GDPR Compliance Roadmap has been developed to help you achieve compliance through focusing on key activities deemed to be essential by the ICO.

These activities are the bare minimum an organisation should carry out and are set out in the 'Essential GDPR Compliance Roadmap' which sets out a step-by-step approach to help an organisation manage its key GDPR obligations.

Step 1: Activity Log

ALL activity carried out should be recorded to demonstrate that the business's compliance process in accordance with 'accountability' a key principle of GDPR.

The activity log must be kept updated and may be required to be seen by the ICO if the need arises.

Step 2: Staff Training

Staff awareness training is an essential compliance requirement, as under Article 43 of the GDPR requires "the appropriate data protection training to personnel having permanent or regular access to personal data."

As human error is at the heart of most data breach incidents, staff training becomes even more important to ensure they understand what is needed to be done in order to remain compliant and avoid simple mistakes.

Organisations are also required to provide evidence of staff training as part of their reporting obligations. So, make sure all training is recorded in the activity log.

The staff awareness programme should be an ongoing process that is reinforced regularly throughout the year especially if there are any significant changes to the legislation and, when new employees join.

Take a look at the ICO's: Training Videos & Resources & Training Checklists for Small & Medium Sized Organisations.

Step 3: Lawful Basis for Processing

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner and, to comply with the accountability principle you must be able to demonstrate that a lawful basis applies.

Furthermore, the individual's right to be informed requires you to inform data subjects about your lawful basis for processing.

This would usually be provided in your Privacy Notice.

Take a look at the ICO's Lawful Basis For Processing & Consent

Step 4: Processor Management

It is mandatory that when a controller uses a processor (a third party who processes personal data on behalf of the controller) there is a written contract that complies with the GDPR.

Similarly, if a processor employs another processor, it also needs to have a written contract in place and proof needs to be provided to the controller.

The contract should set out the responsibilities and liabilities for both parties. If in doubt it is best to seek legal advice.

This audit should list all processors, send compliance questionnaires and ensure contracts are updated in line with the GDPR.

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

Step 5: Data Processing Inventory

The GDPR requires that the controller maintains a record of processing activities under its responsibility, and to make them available to supervisory authorities upon request.

Documenting your processing activities is important, not only because it's a legal requirement, but also because it also supports good data governance and helps demonstrate your compliance with other aspects of the GDPR.

The inventory must be kept up to date and reflect current data processing activities.

Take a look at the ICO's Documentation of Data Processing Activities

Step 6: Operational Protocols

There are seven principles that make up the GDPR and it is essential that these are addressed within your business.

Alongside dictating the need to be fair, transparent and legal, the principles require that you create rules regarding how much data you collect (minimisation), what the data can be used for (purpose limitation) and how long you can keep it for (storage limitation). In practise this will cover CRM systems, emails and HR systems amongst other areas.

The principles also demand that you keep personal data up-todate and accurate, keep it safe and secure, and be able to prove how you are achieving compliance.

Choose the policies that are most appropriate to maintain your organisations data protection obligations.

Take a look at ICO: GDPR Principles for more information.

Step 7: Privacy Information

Privacy notices should be updated to ensure they are GDPR compliant. Please be wary of generic privacy notices as you will need to ensure they have been amended to reflect your business activity. Furthermore, the GDPR requires the information to be provided in concise, easy to understand way and use clear language.

Take a look at the ICO's Privacy Notices Codes of Practice

Step 8: Subject Access Request(SAR)

Under the GDPR individuals have a right to see a copy of the information an organisation holds about them and this is commonly referred to as a SAR, or Subject Access Request.

Since you have only a month to comply and no fee is required to be paid, you will need to set up procedures to enable you to handle the requests.

Depending on the number you are likely to receive you may wish to look at third party software to manage this.

Take a look at the ICO's information on Subject Access Requests & their Subject Access Code of Practice

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

Step 9: Data Breaches

Ensure you have the right procedures in place to detect, report and investigate a personal data breach.

The GDPR places a responsibility on you to notify the ICO of a breach 'where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly.

You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred.

Take a look at the ICO's information on Personal Data Breaches

Step 10: Privacy by Design

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.

The ICO requires organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle.

This 'privacy by design' approach is essential in minimising privacy risks and building trust.

Privacy Impact Assessments (PIAs) or Data Protection Impact Assessment (DPIA) are an integral part of 'privacy by design' and are used a tool to identify and reduce the privacy risks of projects

Take a look at the ICO's guide to Privacy by Design & DPIA's

04
Maintaining compliance

It is essential compliance is maintained and you should carry out an annual audit to ensure your organisation is following good data protection practice and meeting their data protection obligations.

The audit should look at whether your controls, policies and procedures are effective in maintaining your data protection obligations.

It is also important to ensure new and existing staff receive appropriate training to maintain the organisations data protection obligations.

05
Conclusion

Whilst we have tried to simplify GDPR compliance, it is nonetheless a process that will take time to understand and implement.

The compliance journey is best undertaken one step at a time and we hope our roadmap will assist you in achieving this.

Acumenology has produced a series of Business Guides on a variety of topics relevant to starting and running a business.

These can be found at:
www.acumenology.co.uk/business-guides