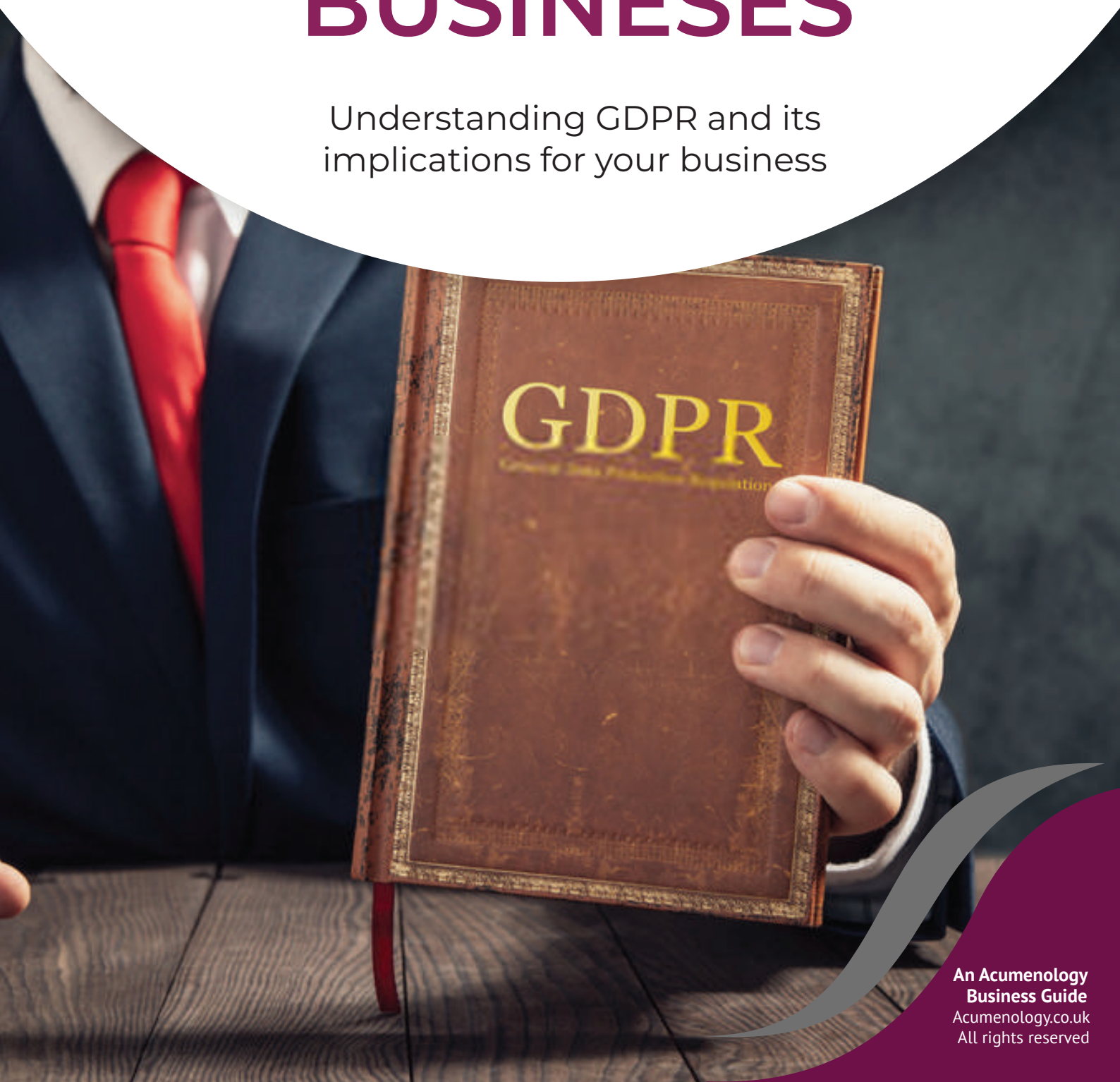
Acumenology

business support

GDPR GUIDE FOR SMALL BUSINESSES

Understanding GDPR and its implications for your business



An Acumenology Business Guide

Acumenology.co.uk

Contents

01

Introduction

There is considerable information easily and freely available on GDPR (General Data Protection Regulation). Though the information may seem complicated and difficult to understand, the ICO website(Information Commissioner's Office) provides a good starting point.

At Acumenology our aim is to help you by providing you with information that is easy to understand.

The purpose of this document is to help business owners and key management get an understanding of GDPR, its requirements, implications for the business and potential consequences of failure to comply.

It will also show you the steps needed to comply thereby allowing you to plan your compliance journey and allocate adequate time and resources.

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

This article was first published on January 2020 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.

02

What is GDPR?

The GDPR is new European legislation that came into force on the 25th May 2018.

It is applicable to ALL businesses and organisations no matter how small, that collect or process personal data of EU residents such as names, addresses, customer lists, employee records and even online identifiers such as a computer's IP address.

It is built around two key principles.

1. Giving citizens and residents more control of how their personal information is collected and processed.
2. Simplifying and unifying regulations across the EU.

The GDPR requires organisations to demonstrate compliance with the six GDPR principles by adopting appropriate policies, procedures and processes to protect the personal data they hold.

This involves taking a risk-based approach to data protection and building a workplace culture of data privacy and security for the entire organisation.

03

Understanding GDPR

With 11 chapters and 99 articles going through the GDPR's requirements can be overwhelming.
To find out more **CLICK HERE**.

To make it easier to understand we can classify GDPR broadly into two categories. **Principles and Rights**.

Principles

The GDPR defines a wide range of requirements that organisations collecting or processing personal data must follow and are based on six key principals.
To find out more **CLICK HERE.**

1. Lawfulness, Fairness & Transparency

Personal data shall be processed lawfully, fairly, and in atransparent manner in relation to the data subject.
Article 5, clause 1(a)

2. Purpose Limitation

Personal data shall be collected for 'specified, explicit and legitimate purposes'.
Article 5, clause 1(b)

3. Data Minimisation

Data collected on a subject should be 'adequate, relevant and limited' to what is necessary for a specific purpose.
Article 5, clause 1(c)

4. Accuracy

Data must be 'accurate and where necessary kept up to date'.
Inaccurate or outdated data should be deleted or amended.
Article 5, clause 1(d)

5. Storage Limitation

Personal data shall be kept for no longer than is necessary.
Article 5, clause 1(e)

6. Integrity & Accountability

Personal data must be protected against unauthorised access to ensure no personal data is accidentally lost, breached, or damaged.
Article 5, clause 1(f)

Rights

The GDPR gives individuals certain rights, these are:
To find out more **CLICK HERE.**

1. Right to be informed

Organisations are required to process information in a fair way and data subjects must be informed if any breach or data loss affects their personal data.

This article was first published on January 2020 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.

2. Right of access

Organisations must provide data subjects with complete access to their personal data if a subject requests it.

3. Right to rectification

When data subjects access their personal data, organisations must provide them with options to change or rectify their personal data without any restriction.

4. Right to erasure

If a data subject demands their personal data to be removed from an organisation's database, the organisation must comply immediately.

5. Right to restrict processing

Data subjects can demand access to their personal data be restricted so the organisation can only access it for certain purposes.

6. Right to data portability

Data subjects must be given the option to transfer their personal data from one vendor to another.

7. Right to object

The data subject has the right to demand that the organisation stop processing their personal data for any reason.

8. Rights in relation to automated decision-making and profiling

Data subject have the right to demand theorganisation stop processing their personal data if it is being profiled for other marketing activities.

04

Who does the GDPR affect?

GDPR applies to any business that collects and processes the personal data of EU citizens.
This includes customer, supplier, partner and employee personal data.

It also applies to organisations not established in the EU but offer goods or services to data subjects within the EU. Thus, if you're collecting any of this data no matter how small, you will need to comply with the GDPR.

Some examples of personal data your business may collect and thus would fall under the scope of GDPR are as follows:

- Customer database
- Supplier database
- Sales database
- Customer feedback form
- Employee information
- CCTV
- Location data (gathered from an app or website)
- Loyalty scheme records
- Health information
- Financial information
- Online identifiers such as IP addresses (when someone visits your website.)

05

What are the implications of GDPR for a business?

The new legislation requires all businesses & organisations no matter how small to transform the manner in which they approach data protection.

This means changing existing policies, putting in place new processes and ensuring all staff are adequately trained to ensure compliance.

GDPR includes a new accountability principle that states that data controllers (A person(s) or entity that determines the purpose and the manner in which any personal data is to be processed), must be able to demonstrate compliance with the six principles.

It is not enough to comply; you have to be seen to be complying by putting in place a range of processes that are proportionate to the complexity of the processing and size and nature of the business.

06

Consequences of failure to comply

Failure to comply with the GDPR through either 'administrative failures' or personal data breaches may result in a regulatory investigation which in itself can be very time-consuming, and a potential fine.

However, it should be noted that not all infringements will lead to the serious fines.

Beside the fines, the ICO also has a range of corrective powers and sanctions which can be imposed on a business.

Non-compliance could lead to any or all of the following:

1. Administrative fines

These are discretionary rather than mandatory, must be "effective, proportionate and dissuasive", and are decided on a case-by-case basis.

There are two tiers of fines:

Tier 1 - Up to €10 million, or 2% annual global turnover – whichever is higher.
For infringements of the organisation's obligations, including data security breaches.

Tier 2 – Up to €20 million, or 4% annual global turnover – whichever is higher, for infringements of an individual's privacy rights.

2. Liability for damages

Individuals have the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR.
This could potentially be very damaging as it may open the door for claims from 'no win no fee lawyers'.

3. Reputational damage and loss of consumer trust

How would your business cope in the event of noncompliance?

07

What do you need to do to comply?

Compliance under the GDPR is a journey that involves a change in the culture and the way your business deals with personal data be it for your customers, staff or suppliers.

It is not a tick box exercise

Since the GDPR places great emphasis on 'accountability' to demonstrate compliance, it is essential that you develop a planned approach' and allocate sufficient resources.

At Acumenology we have a thorough understanding of the challenges small businesses face have developed a '5 Phase GDPR Compliance Roadmap'.

Phase 1. Understand GDPR

Create awareness amongst key decision makers, develop a plan and provide training

Phase 2. Discover & Identify

- Create an information audit on data you hold for customers, staff and suppliers and assess risks.
- Gap analysis - assess compliance against GDPR requirements

Phase 3. Implement changes

- Implement systems and processes stated in the Gap Analysis including physical, technical and administrative safeguards.
- Ensure consent is managed correctly, privacy notices updated, and processors are compliant.
- Ensure Subject Access Requests & Data Breach processes are in place.

Phase 4. Develop Controls

Develop, enhance and manage controls such as:

- PIA's (Privacy Impact Assessments) which are required under GDPR
- Data minimisation, retention and control
- Data integrity & quality
- Data breach incident response plan.

Phase 5. Maintain compliance

Ensure on-going compliance through an annual audit, new staff training and the services of a shared DPO if considered necessary.

08

What happens in case of a data breach?

A data breach is more than just being hacked or losing personal data. It also applies to the loss of personal data held in any form – not just electronic.
Thus, it is important to understand the importance and consequence of a data breach under the GDPR as it is inevitable that organisations will have at the very least a minor breach.

When should a data breach be reported

A personal data breach should be reported to the ICO within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

Some examples of personal data breaches can include:

- Access to personal data by an unauthorised third party
- Sending personal data to an incorrect recipient.
- Devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

To find out more **CLICK HERE.**

09

Is a data protection officer required?

It is only mandatory to appoint Data Protection Officer (DPO) if you are a public authority, or if you carry out certain types of processing such as 'regular and systemic monitoring of data subjects on a large scale'.

To find out what activities require a DPO **CLICK HERE.**

Whilst it is unlikely that most small businesses would require the services of a DPO, you may as 'good business practice', wish to consider using the services of a Data Protection expert to manage your risk in the same way as businesses use external HR, Accountants or Health & Safety professionals.

Role of a DPO

The role of the DPO is to help a business comply with data protection regulations and to avoid risks related to processing personal data whether as a 'controller' or 'processor'.

Their tasks are:

- To inform and advise a business to their data protection regulations.
- To monitor compliance including assignment of responsibilities.
- Raise awareness, train staff and advise on Data Protection Impact Assessments as required.
- Be the point of contact for data subjects and liaise with the ICO on data breaches.

This article was first published on January 2020 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.

The DPO could be an individual within your company or, an external 'DPO as a service' provider.
However, it is essential they be independent, adequately resourced and are able to report directly to senior management.

They must also have "expert knowledge of data protection law and practices" in order to perform their duties.

10
Conclusion

Having read through the information contained herein you should now have a better understanding of the GDPR, its requirements, implications for your business and the compliance process.

You should also ensure all key decision makers have also familiarised themselves with the information in this document.

It is important to recognise that GDPR compliance involves a change in culture and processes.

Think of it is Highway Code for personal data privacy. The Highway Code does not teach you how to drive. It provides a framework of rules and regulations to ensure your own safety and the safety of other users.

Your next step should be to develop a plan, allocate adequate resources and set a timeline.

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