GDPR Myths for Small Businesses

Executive Summary

- The UK GDPR applies to nearly every business operating within the UK, as well as all types of business models regardless of their size.
- You do not have to be a large company to fall under the jurisdiction of this law.
- The purpose of the GDPR is not just to have a paper trail, but rather to promote the fair and secure handling of individuals' personal information.
- Most small businesses will not require a fully dedicated Data Protection Officer (DPO).
- Organisations only need to develop policies and have documentation that is appropriate for their level of risk and how big they are.
- While fines are a possibility, the Information Commissioner's Office (ICO) tends to work with business to educate and help rather than penalise or set penalties. They focus mostly on educating, working with and helping improve SMB compliance efforts.
- If approached in a practical manner, UK GDPR compliance can be achieved in 30 days.
- Implementing good data protection practices will reduce your business risk, improve trust, and prevent companies from incurring expensive breaches.

Who This Guide Is For

This guide was written for:

- UK businesses with 1–50 employees
- Owner-operated companies
- Businesses who are starting up or expanding
- Professional services, trades, retail, consulting, and e-commerce businesses
- Directors and managers (who may not be technically oriented) who find this legislation intimidating.

What You’ll Achieve

At the end of this guide, you can expect to learn:

- What the requirements of the UK GDPR actually are.
- What myths and misconceptions exist in relation to legal requirements.
- The minimal practical standard of the UK GDPR compliance will be for small to medium enterprises.
- A 30-day plan outlining your actions will be produced.
- You will feel more comfortable than afraid of your duties under the legislation.

Why GDPR Confusion Exists (UK Context)

The GDPR rules were introduced in 2018 and were incorporated into UK law when the UK left the EU (referred to here as "UK GDPR"). The body that regulates the GDPR within the UK is the Information Commissioner's Office (ICO). There appears to be confusion around the GDPR rules for a number of reasons:

- Media stories have focused on very large companies receiving very large fines.
- Consultants often over-complicate the requirements.
- Templates and jargon have added unnecessary complexity to the process.
- Small companies believe they are either completely exempt or are at high risk of being penalised under GDPR.

The reality sits somewhere in the middle. The ICO's guidance consistently states that compliance with the GDPR will be proportionate to your organisation's size, scope and level of risk.

15 Common GDPR Myths (Myth vs Reality)

Myth 1: "GDPR doesn't apply to small businesses."

Reality:

If your organisation processes personal data in any way, shape or form, then you are subject to the GDPR regardless of how large your organisation is.

Personal data includes:

- Employee records
- Customer names and contact details
- Email addresses
- CCTV images
- Supplier contact details

There is no small business exemption.

Myth 2: "We need to appoint a Data Protection Officer."

Reality:

Most small businesses do not need to have a formal Data Protection Officer (DPO).

A DPO is only required when:

- You are engaging in widespread monitoring activities;
- You are processing high volumes of sensitive personal information; or
- You are a public authority.

Most smaller organisations will simply need to appoint someone who has responsibility for ensuring your compliance with the GDPR.

Myth 3: We Need To Comply With The ICO Because Of (The) GDPR

Reality:

The ICO Registration (Data Protection Fee) Was Established Prior To (The) GDPR. Businesses That Process Personal Data Are Generally Required To Pay An Annual Fee, But This Is Separately From The Cost Of Compliance (With) The GDPR.

Myth 4: We Need Written Consent For Every Activity That We Undertake.

Reality:

Consent Is One Of Several Lawful Bases For Processing Personal Data. Lawful Bases Include:

- Contract
- Legal Obligation
- Legitimate Interests
- Vital Interests
- Performance Of A Public Task

Most SME Activity Will Be Based On Contractual Or Legitimate Interest Rather Than Consent.

Myth 5: GDPR Does Not Allow Us To Send Emails To Clients.

Reality:

You Can Send Emails To Clients If You Have A Lawful Basis To Do So. The Rules Relating To Marketing Are Primarily Governed By PECR (The Privacy And Electronic Communications Regulations) As Opposed To The GDPR.

Myth 6: We Must Delete All Data After One Year.

Reality:

- Under The GDPR Data Retention Must Be:
- Lawful

- Necessary
- Proportionate

Some Categories Of Financial Records Must Be Kept For A Minimum Of 6 Years For HMRC Purposes. Therefore Retention Periods Will Be Dependant On The Legal Business Needs.

Myth 7: We Are Required To Have Complicated Documentation.

Reality:

An SME Requires Adequate Documentation Which Is Proportional To Its Size And Scale Includes;

- Privacy Notice
- Data Protection Policy
- Basic Data Map
- Responsibilities For Responding To An Incident

All Other Documentation Should Be Kept To A Minimum (For Example 200 Page Document).

Myth 8: Fines for Violating GDPR Are Automatic

The ICO takes proportionate steps to penalise violators of the law.

An ICO fine results when:

- There is negligent behaviour,
- Repeatedly not complied,
- Hurtful non-compliance, or
- Lack of cooperation.

Small businesses that have made a good faith effort and are accountable may get treated differently.

Myth 9: If We Use Cloud Services, the Cloud Service Provider Will Be Responsible

The data controller remains responsible regardless of the use of cloud services.

Typical cloud services are data processors, and you are still responsible as the data controller.

To be compliant with GDPR, you must verify:

- A data processing agreement is in place,
- Adequate safeguards exist.

Myth 10: We Must Encrypt Everything

GDPR only requires technical and organisational measures to protect personal data. However, encryption is strongly recommended for the following:

- Laptops,

- Portable devices,
- Backups, etc.

Encryption is not mandatory in every instance according to the law.

Myth 11: All Breaches Will Result in a Fine

Not every breach results in a fine.

When a data subject has a risk to their rights and freedoms, they will need to assess the risk and notify ICO within 72 hours from the time of breach.

Myth 12: GDPR Is Primarily About IT

The GDPR also affects the following types of businesses/process descriptions:

- HR processes,
- Contractual agreements,
- CCTV surveillance,
- Marketing, etc.
- The GDPR is not just a technical issue.

Myth 13: "Our organisation is not big enough to be targeted."

Reality:

- Data breaches stem from:
- Human Error
- Weak Passwords
- Lost Devices
- Phishing

Small and Medium Enterprises often experience these breaches.

Myth 14: "We need expensive consultancy firms."

Reality:

You can meet many of your business's security needs internally with the use of templates and guidance.

Having a professional work with you can be helpful but not necessarily required.

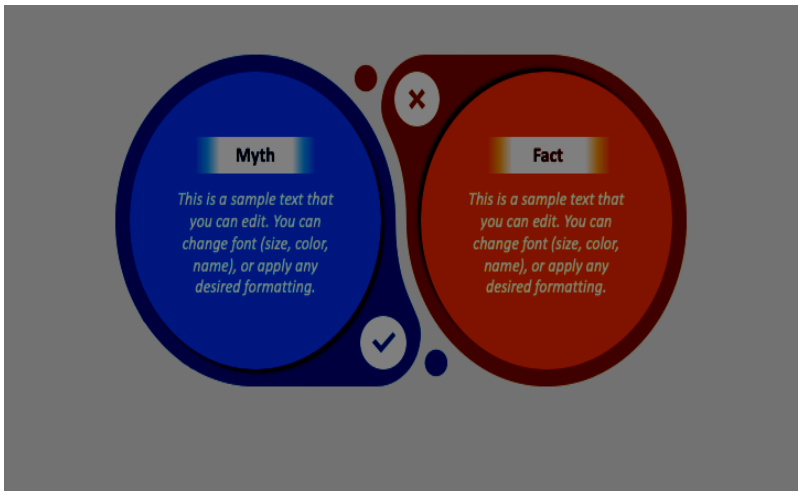
Myth 15: "GDPR compliance is a project."

Reality:

GDPR compliance is an ongoing process that requires:

- Ongoing employee training

- Regular policy reviews
- Security updates
- Ongoing continued monitoring of incidents



What Small Businesses Actually Must Do

The basic minimum level of compliance to be met by most UK small and medium enterprises (SMEs) is as follows:

Identify what Personal Data you hold:

- An initial disclosure that lays out what employee data exists
- A second based on individual customers, marketing and promotional lists
- Identify where the Personal Data is stored
- Identify who has access

Have a Privacy Notice:

The Privacy Notice will typically accompany the data itself and be published on the website, customer-facing materials and includes, amongst other things:

- The type of data to be collected
- The reason it will be collected
- The lawful basis for collecting that data
- How long the data will be retained for
- Contact details for your Information Commissioner's Office

Pay the Information Commissioner's Office Data Protection Fee:

To find out if you are required to register and pay the fee please check the Information Commissioner's Office website.

Have minimum Standards for Security controls:

Minimum Security controls should include the implementation of:

- Strong passwords
- Use of Multi-factor authentication (MFA)
- Use of device encryption and antivirus/EDR
- Use of backup systems

Have a data breach protocol:

A business needs to understand:

- Who would investigate a data breach?
- How would the business assess the risk of a data breach occurring?
- When should the Information Commissioner's Office (`ICO`) be notified?
- What contact method should a business use to notify affected individuals of any data breaches?

Staff Awareness:

Basic annual training of staff which should include:

- Awareness of Phishing attempts
- Handling Personal Data securely
- What to do in the event of experiencing an incident?

Simple 30-Day Compliance Checklist

Days 1–10: Awareness & Mapping	Days 11–20: Security & Documentation	Days 21–30: Governance & Training
• Identify the types of personal data you hold • Confirm the legal bases upon which you rely to process personal data • Update your privacy notice • Confirm your ICO registration	• Implement MFA • Encrypt all laptops • Review access rights • Document your breach procedure	• Train all employees in their data responsibilities • Review all contracts with third-party processors • Create a simple schedule for retaining documents • Schedule an annual review of all data protection practices and procedures

FAQs

1. **Do independent contractors have to conform to the General Data Protection Regulation (GDPR)?**

Yes, if you are processing personal data.

2. **Is the GDPR still in force after the UK's exit from the EU?**

Yes, the UK has GDPR.

3. **How long do we need to report a data breach?**

You need to report it within 72 hours if you believe it poses a risk.

4. **What classifies as personal data?**

Any data being processed that will identify a living person.

5. **Do employers have to obtain consent before processing employee records?**

Generally, no. Processing employee records is generally based on either the contractual basis or a legal requirement.

6. **Will I need a written contract with the suppliers that provide services to me?**

Yes, if your supplier processes personal data on your behalf, you will need a written contract in place with them.

7. **Do I need to have a Data Protection Officer (DPO)?**

It is rare for small and medium-sized enterprises (SMEs) to retain a DPO.

8. **How long should we retain CVs?**

The retention period will depend on the lawful basis for the recruitment process and your recruitment/hiring schedule.

9. **What are the possible consequences of not complying with the GDPR?**

You might receive complaints about your company, be subject to an investigation by the Information Commissioner's Office (ICO), and receive negative publicity that could harm your reputation.

10. **Is the GDPR simply a way for authorities to impose fines?**

No, it is designed to help organisations manage and protect personal data responsibly.

About This Guide

This guide has been prepared by the **Computer Support Centre**, a data protection and cyber security consultancy assisting small and medium-sized enterprises in the UK for the last 15 years; we focus on providing practical, proportionate compliance solutions for small medium enterprises while protecting your customers' personal information and keeping administrative burdens to a minimum for busy business owners.

We aim to reduce unnecessary fear, clarify any true legal obligation, and provide clearly worded, actionable advice to assist in compliance with UK GDPR and that small medium enterprises in the UK can feel confident in implementing.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

Conclusion

To conclude, GDPR should not be perceived as complex and/or scary for small businesses in the UK; for the majority of small/medium-sized enterprises (SMEs), following simple common sense is all that is required to comply with GDPR regulations. Common sense would suggest that SMEs should have an understanding of their reasons for collecting personal information and how to keep it secure; they should also have an adequate understanding of their obligations to notify data subjects of the purpose(s) for which they hold personal information and the period(s) during which they will retain that data, and that the Law is based on risk and therefore an SME's expectations concerning applicable standards should be reasonable and not perfectionist in nature.

By developing straightforward policies, implementing basic cybersecurity controls, creating staff awareness and documenting procedures, small businesses will be able to fulfil their obligations under the UK GDPR confidently. The Information Commissioner's Office has previously stated that implementing practical and appropriate measures to comply with the UK GDPR is key; therefore, by having a structured approach to achieving compliance with the UK GDPR, small businesses can manage their compliance obligations and even benefit their business by establishing trust from their customers.