# GDPR BASICS EVERY UK BUSINESS SHOULD UNDERSTAND

*A plain-English guide to GDPR obligations for UK small businesses*

*For UK business owners, directors & managers (1–50 staff)*

*UK GDPR & Data Protection Act 2018 explained*

*Practical checklists & real-world examples*

*Non-legal, non-technical guidance*

**Prepared by**

**Computer Support Centre**

https://computersupportcentre.com

# GDPR Basics Every UK Business Should Understand

## Executive Summary

- Businesses in the UK are subject to the General Data Protection Regulation (GDPR), regardless of their size.
- The aim of the GDPR is to ensure that businesses handle customer data legally, ethically and safely, not just to fill in forms or meet requirements.
- While small businesses shouldn't strive for perfection, they do need to take reasonable steps to comply with the GDPR.
- To collect and retain personal data, businesses should only collect what is needed.
- Although all individuals have rights based on the GDPR, the majority of requests are relatively simple to handle.
- GDPR does not prevent normal business activity when applied correctly.
- The purpose of this guide is to provide small and medium-sized enterprises (SMEs) with practical information on how to achieve compliance, rather than to provide a detailed legal explanation.


## Who This Guide Is For

This guide is specifically designed for Business Owners and Directors located in the UK, Office/Personnel/Human Resource and Operations Managers who manage smaller teams (1-50 employees) and Non-Technical and Non-Legal Readers, so it is particularly useful to people working within Professional Services, Retail, Trade, Charity, and Small Office sectors.

## Who This Guide Is Not For

This guide is not:

- Legal Advice
- An alternative to a lawyer or data protection attorney
- A very technical guide on how to implement security in your computer system
- An assurance of being certified to comply with legal regulations

**Disclaimer:** This guide is for general information only and does not constitute legal advice.

## What GDPR Is

As part of the Data Protection Act 2018 (along with UK GDPR), GDPR is designed to help safeguard people's personal information, and it attempts to hold organisations accountable for the proper handling of personal information.

Basically, under GDPR, organisations must:

- Explain what information they collect from individuals.
- Tell you what they are doing with that information and why they need to collect it.
- Have reasonable safeguards in place to ensure the security of that information.
- Not retain any personal information longer than is necessary to fulfil their obligations under the Data Protection Act.
- Honour each individual's rights regarding their data.

Ultimately, GDPR is meant to create an environment of trust, not to hinder business activities.

## Does GDPR Apply to My Business?

Generally speaking, yes.

The GDPR applies to your business if you:

- Provide employment.
- Have customers or clients.
- Maintain personal data, payroll information, or email lists.
- Utilise computer technology or information technology (IT) service providers, or payroll services.

If you process any personal data, GDPR is likely to be applicable to you.

## The 7 GDPR Principles, Explained Simply

The GDPR is a series of rules, which enforce the effects of Fair Practices in processing of personal data.

| Principle | What It Means in Practice |
|---|---|
| **Lawfulness** | you process personal data based on a legitimate basis. |
| **Fairness** | you do not process personal data in a manner that is unexpected or unfair to individuals. |
| **Transparency** | you provide individuals with notice of your processing activities |
| **Purpose limitation** | you collect, use and disclose personal data for the purposes for which you collected the data. |
| **Data minimisation** | you only collect personal data that is necessary for your processing. |
| **Accuracy** | you keep personal data accurate, complete and up-to-date as necessary. |
| **Storage limitation** | you do not keep personal data indefinitely. |
| **Security** | you take steps to protect personal data from loss or misuse. |


## Lawful bases for processing

**Why it is important:**

Every time you perform one of your main processing activities ("Sending Invoices"; "Running Payroll"; "Sending Marketing Emails"), you should have at least one lawful basis for processing. The ICO specifies that there is a lawful basis for each processing of personal information under Article 6, and it must be a lawful basis before an entity can process personal information.

**SME's view of the six lawful bases**

- **Contract:** A lawful basis of processing is needed when providing a service or fulfilling an agreement (to send Quotes, Deliver Goods, and Bill Customers).
- **Legal Obligation:** An Organisation is legally required to keep certain records of their payroll activity (including Payroll, Tax/VAT) and to comply with Employment Law duties.
- **Legitimate Interests:** Processing can be done if it has a legitimate business reason as long as it does not infringe upon an individual's right to privacy, e.g., some B2B Marketing, Basic Fraud Prevention. The ICO states that to prove legitimate interest the business must demonstrate a three-part test (Purpose, Necessity, Balance).

- **Consent:** An Organisation must have a clear consent from an individual for their specific purposes of processing (usually Marketing / Optional Extras).
- **Vital Interests:** Processing for the protection of the life and death of individuals is a rare lawful basis for SMEs.
- **Public Task:** The lawful bases for processing for non-public authorities is also a rare lawful basis for SMEs.

### Common requirements for SMEs:

- List your main processing activities (5–15 is fine)
- Each processing activity will require a Lawful Basis.
- The Privacy Notice must reflect the information listed above in plain English.

**Practical Examples:**

- **Invoices:** Lawful Basis Contract + Legal Obligation
- **Payroll:** Lawful Basis Legal Obligation
- **Customer Support Emails:** Lawful Basis Contract / Legitimate Interests (depends on the situation)
- **B2B Newsletters:** Lawful Basis Consent or Legitimate Interests (depends on the situation and PECR considerations).

## Roles & responsibilities (controller vs processor)

**Why it is important:**

The difference between a Data Controller and a Data Processor is an important piece of information for small and medium enterprises (SMEs) to understand, as it will affect their obligations as well as what is required in supplier contracts.

**Simple definitions**

- Data Controllers decide why and how personal data is processed.
- Data Processors process personal data for Data Controllers, and follow the instructions of the Data Controllers.

**Most SMEs are controllers for:**

- Staff Data
- Customer Data
- Supplier Contact Dat**a**

Additionally, several SMEs remain Data Controllers under the use of Cloud Services, as they still decide the purpose for which personal data is stored (for example, "to store Human Resource Files' on Microsoft 365").

### UK SMEs (typically) identify their Key Data Processors:

- Identify key processors: payroll provider, IT support/MSP, CRM, email marketing tool, cloud storage
- Ensure you have appropriate contracts / terms (often called “data processing terms”)
- Check where data is stored and who can access it (especially admin access)

### Practical examples

➢ **Payroll Bureau:** typically considered Data Processor.

➢ **IT Support/MSP:** normally Data Processor for Support Activities.

➢ **Accountant:** potentially Data Controller for his/her Services.

## Individual rights (what businesses must support)

**Why it is important:**

Individuals have ownership of their Personal Data. While small and medium businesses may not have in-house legal assistance, they will need to establish processes to respond to these requests, so their business does not come to a stop while they try to fill them.

### Main Rights:

- Subject Access Request (Access)
- Right to Rectification (Correct Mistakes)
- Right to Erasure (In Limited Situations)
- Right to Restriction
- Right to Data Portability
- Right to Object
- Rights Regulating Automated Decision-Making (Less common for Small or Medium Businesses)

### Subject Access Requests (SARs) — What Small and Medium Businesses Need To Know

Businesses are generally required to respond without delay and to comply with a request within 1 month of receipt of the request, with the possibility of extending the 1 month limit in certain situations (e.g., complex requests).

**What Does a Small or Medium Business Need To Do?**

- Appoint a "Request Owner" (Operations Director).
- Verify Identity in a Reasonable Manner.
- Conduct Searches in All Relevant Systems (email, HR folder, CRM/Finance Systems).
- Provide Data in an Easily Understood Format.
- Maintain a Simple Log of Request Date and Actions Taken.

**Practical Example**

A customer emails with the following request: "Please send me all information you have about me."

In this case, the following will need to happen:

- Log Date of Request.
- Verify Identity.
- Export Data from CRM System as well as relevant emails/Invoices.
- Check if Any of the Data Is Subject to a Reasonable Basis for Withholding (unlikely but possible).
- Respond Within 1 Month.

# Security & data protection (high-level, practical)

## Why it is important:

DPR pain can often be traced back to preventable incidents like lost laptops, shared passwords, mistakenly sent emails, improperly configured access controls, and poor supplier practices.

## What UK SMEs typically need to do (practical baseline)

## Access Control

- Use individual/user names and/or accounts
- Implement multi-factor authentication - especially for email accounts
- Define access controls based on 'least privilege' requirement (admins only have full rights when necessary).

## End-user Device Protection

- Laptops should have encryption enabled (BitLocker or FileVault)
- All end-user devices should have screen locks activated and require a strong PIN code
- Use a secure password manager (while this is not a legal requirement, it is highly recommended)
- Dispose of end-user devices & paper securely.

## Backups and Availability

- Have backups that are stored separately from your main systems.
- Test the restoration of backups at least once annually, but every 3-4 months is recommended.
- Plan how to operate during an IT outage (see your BCP policy).

## People

- Basic training to identify phishing attempts and how to handle Personal Data.
- Encourage a "Stop and Check" culture around unusual requests.

### Practical examples

- **Professional Services:** Limit access to the clients' folders and Audit who can access sensitive matters.
- **Retail:** Limit the number of POS/Admin accounts and Manage who has access to the Customer Orders.
- **Small Office:** Do Not Forward Business Mail to a Personal e-mail address.

## Data breaches & incident response (SME-focused)

### Why it is important:

Data Breaches Occur. What Matters is How You Respond (Contain, Risk Evaluate, Determine if Reporting is Needed, and Learn).

Under the ICO: If a Breach has Met the Reporting Threshold, You Must Report It Without Delay and Within 72 Hours of Discovering It.


### What Is a Personal Data Breach?

A security incident where the personal data was destroyed, lost, altered, or disclosed lawfully by accident or was accessed unauthorised.

### Examples of Personal Data Breaches for SMEs

- Stolen Laptop with customer file
- Email containing personal data sent to the wrong person
- Compromised email with unusual forwarding rules
- Shared HR spreadsheet publicly by mistake

### What UK SMEs typically need to do

- Have a 24-72 hour Action Plan
- Maintain a Security Breach Log Even if the Incident Does Not Need to be Reported
- Know Who Has the Authority to Decide to Report
- Have an IT/MSP Escalation Path

## Documentation & Accountability (What SMEs Actually Need)

There are some documents you must create if you run an SME.

**These include:**

- Privacy Notice
- Data Retention Policy
- Data Processing Agreements
- Breach Response Procedures
- Basic Data Map

These documents can be simple, they do not need to be unwieldy or elaborate.

## Minimum GDPR Basics for SMEs (Checklist)

☐ Privacy Notice Published.

☐ Identified LLB's & Lawful Basis of Processing.

☐ Defined Periods to Retain Data.

☐ Staff are Aware of their Responsibilities.

☐ Instance of the Organisation has been Secured and Encrypted.

☐ Documented Breach Containment Procedures.

## Breach Response Checklist (First 24–72 Hours)

☐ Contain the Incidence.

☐ Evaluate the Risk to Individuals.

☐ Document What transpired.

☐ Determine if Notification to ICO is Required.

☐ Communicate, IF Necessary.

## Simple data mapping example (who, what, where, why)

Example: small trades business (15 staff)

| Who | What personal data | Where stored | Why (purpose) | Lawful basis (typical) | Shared with |
|---|---|---|---|---|---|
| Customers | Name, address, phone, job notes | Job system + email | Deliver service & invoice | Contract | Payment provider, accountant |
| Staff | Payroll, bank details, emergency contact | Payroll system + HR folder | Employ & pay staff | Legal obligation/contract | Payroll provider |
| Prospects | Name, email | CRM | Quotes & follow-up | Legitimate interests/consent | Email platform |

Keep it short and real.

## FAQs

**Is GDPR applicable to small businesses?**

Yes, the size of a business does not eliminate its responsibility to comply with GDPR.

**Do all small and medium-sized enterprises (SMEs) need to have a Data Protection Officer?**

No, the majority of SMEs are not required to appoint a Data Protection Officer.

**Can I store data without a good reason?**

Storing data for no good reason is not allowed.

**What happens if I accidentally collected or stored data incorrectly?**

Showing that you took reasonable attempts to prevent mistakes from occurring is important.

## Final soft CTA

I offer a GDPR readiness or Data Handling review (which is not a legal review but rather the types of things we would generally do to prepare for GDPR) Here are some things typically included in a good Review:

- An example of a Data Map (Where your data is located, which categories it falls under and Why).
- Your Data Retention Plan; (When will you delete your data (Do Not Keep Forever)).
- The Suppliers from whom you receive services that may be a risk to you (Payroll, Cloud services, IT Support).

- Security Basics Examples (Use MFA to access information, You must encrypt all sensitive data, Keep Backups, Provide Employee Training);
- reparing for SAR/Breach Response (Simple Playbooks);

If you prefer, please send Me the Type of Business (10 Person Accountancy, Retail Store, Plumber), along with Tools Used (Microsoft 365, Google, CRM); I would then create a Minimum Baseline Checklist and Data Map Example based on your specific needs.

## About This Guide

This guidance has been produced by Computer Support Centre, a UK Data Protection and IT Advisory company that assists small businesses in implementing practical, real-world compliance solutions.

We saw the need for this guide after speaking with many small business owners who find GDPR overwhelming, particularly as many interpret it in a legal context and view it as such. The truth is that the vast majority of the requirements found within GDPR are concerned with sound practices for handling data properly, the formulation of good quality procedures and basic security, and not the complex legalities of GDPR.

The purpose of this document is to provide owners and managers with an easy-to-read reference tool that breaks down the key elements of the UK GDPR so that they can easily grasp what is important to their organisations, what seems to have been misinterpreted in the past, and how GDPR fits in to the normal business day-to-day activities of the organisation, without using scare tactics or adding unnecessary complexity.

It should be noted that this document is for general use only, and as such does not constitute legal advice.

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



# Conclusion

The GDPR is about managing people's personal data with transparency and security, not about preventing businesses from trading.

For the majority of small businesses in the UK, it does not mean having to achieve absolute compliance or be overwhelmed with impractical levels of paperwork, but rather it means creating and using appropriate levels of controls across people, processes, and technology that are consistent and widely understood.

By concentrating on the foundations of managing your customers' data that is, understanding what data you hold on your customers, how long you hold it for, and how you protect it all businesses can develop a strategy that will enable them to meet their obligations while at the same time increase customer, employee and partner confidence.

Therefore, rather than seeing the GDPR as a hindrance to growth, you should view it as an integral part of good business practice.