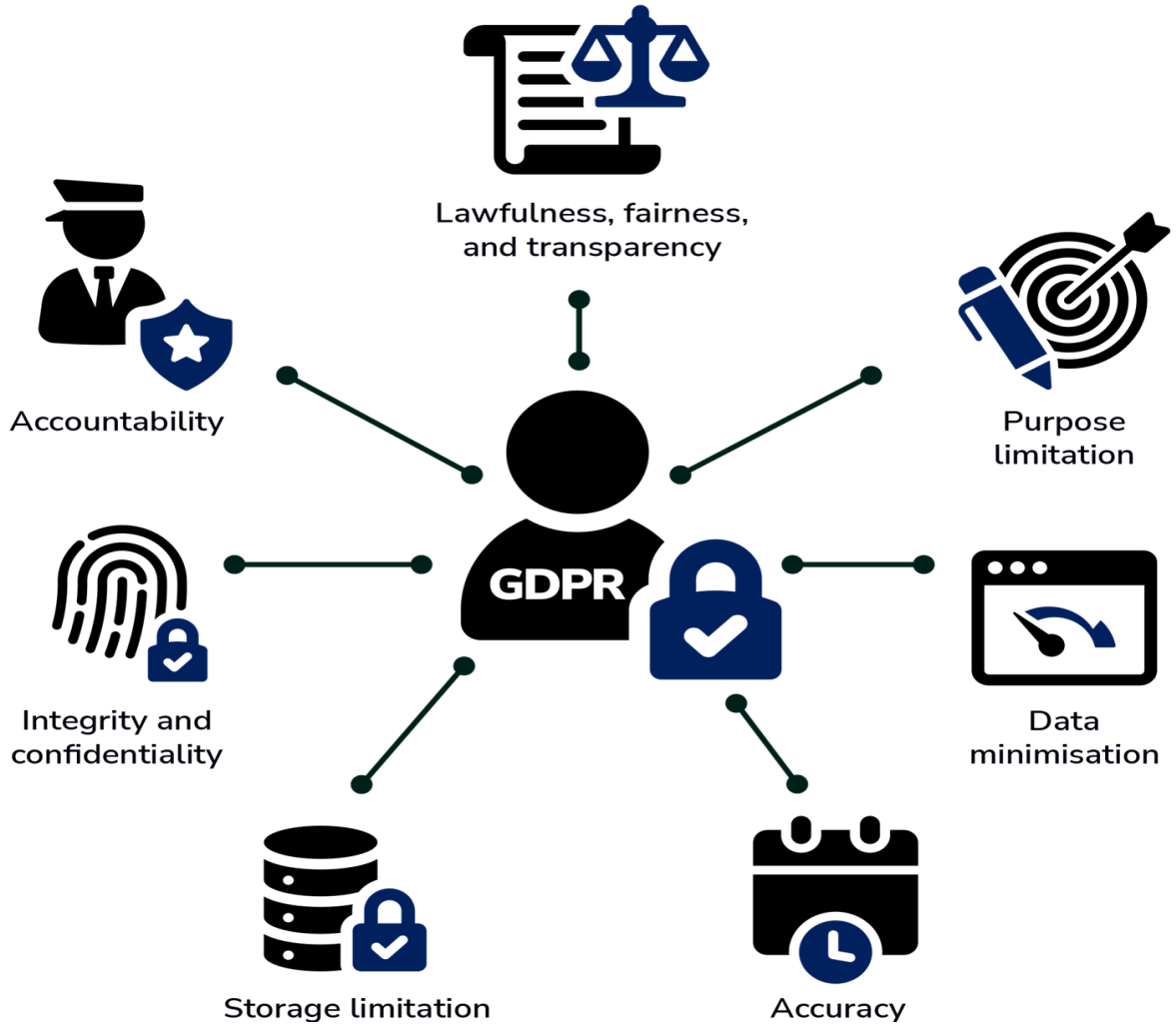
# IT security responsibilities under GDPR

## Executive Summary

- Security in terms of GDPR is considered reasonable and based on risk, but not perfect.
- No specific technology or tool is mandated by GDPR; it is left to the individual data controller to determine what is appropriate for them.
- For a controller to determine what is appropriate, they need to assess the risks associated with processing, their size, and types of data processed.
- Most security breaches of GDPR are typically basic controls failures and not advanced attacks.
- Evidence and accountability must be equally important to organisations as controls.
- Control of user access and user management are clearly expected of all organisations under GDPR.
- Controllers are required to provide backups and ensure their systems are available, these are not simply an IT best practice.
- The response to a breach must focus on speed, clarity and evidence, not blame.
- Employee awareness training as a part of GDPR compliance is mandatory.
- It is important not to over-engineer your security to achieve compliance with GDPR.



## Who This Guide Is For

This guide is intended especially for the following audiences in the UK:

- Micro to medium-sized businesses and charities
- Business owners, directors/trustees to whom it applies
- Those responsible for managing personal data
- IT leaders/operational decision makers
- Non-legal professionals who want practical information without needing to read through all of the relevant legislation.

## GDPR & IT Security Explained

In the UK, personal data (such as names, email addresses, and health-related) is protected by UK GDPR (General Data Protection Regulation), which is the UK's Data Protection Act 2018 amended from GDPR based on EU regulations after Brexit. Article 32 of the GDPR mandates that "IT Security" involves the use of reasonable measures to protect data from loss, unauthorised access, or damage. This may include implementing passwords, regularly backing-up data, training personnel, and regularly reviewing procedures for preventing data breaches.

Establishment of the UK GDPR and Data Protection Act provides organisations with an assurance that their employees will handle information in a secure manner so as not to harm individuals, and ultimately build confidence in the handling of personal data. While some small business owners may feel overwhelmed thinking that the UK GDPR requires them to have "perfect" measures to comply with the Law, there is a focus on practicality. Appropriate or commensurate measures to protect personal data should be based on risk (e.g., handling sensitive health-related information) as well as available technology and cost.

Personal data is defined as anything that identifies an individual, special category data includes sensitive or health-related information, and protection measures must include additional diligence.

## Roles & Responsibilities Under GDPR

### Controller vs Processor

Covers:

- What a data controller is
- What a data processor is
- Shared responsibility explained simply
- Why contracts matter, but don’t replace security

Includes:

- SME examples (outsourced IT, cloud providers)
- Common misunderstandings

## 1. Lawful Processing & Data Protection Principles (Security Focus)

**Covers:**

- The integrity and confidentiality principle
- The availability principle
- Data minimisation from a security perspective

**Examples:**

- A small business with a customer database
- A charity with donor records

**Common mistakes:**

- Collecting too much data
- Leaving old, unsecured systems in place

## 2. “Appropriate Technical & Organisational Measures”

**Risk-Based Security Explained Simply**

**Covers:**

- Assessment of what "appropriate" means
- Factors Regulatory Authorities Take Into Consideration:
- Data Type
- Amount of Data
- Risk of Harm
- Size of Organisation
- The Difference Between "Best Practices" vs. Legal Obligations

**Examples:**

- Micro vs. Small and Medium-Sized Enterprises (SMEs)
- Special Education Needs and Disabilities (SEND) and Handling Special Category Data

**Common mistakes:**

- Assuming GDPR Requires Only Enterprise Level Tools
- Blindly Copying from Large Companies Without Understanding Why

## 3. Access Control & User Management

**Covers:**

- Unique User Accounts

- Least Privilege
- Onboarding/Off boarding/Transfers of Employees
- Admin Access Separation

**Includes:**

- Access Control Checklist (mandatory)
- Examples from SMEs

**Common mistakes:**

- Using Shared User Accounts
- Overlooking Departed Employees
- Providing Unnecessarily High Levels of Admin Rights

## 4. Device & Endpoint Security

**Covers:**

- Mobile Devices, Desktops and Laptops
- Employee versus Personal Use
- Management of Patch History
- Risk of Having Devices Stole

**Examples:**

- Working from Remote Locations
- Bring Your Own Device (BYOD) Model

**Common mistakes:**

- Windows Patches that are not installed
- Incomplete inventory of devices
- No remote wipe capability

## 5. Encryption & Data Protection

**Covers:**

- A Direct Response to The Question If GDPR Requires Encrypted Data
- Explanation of Encryption at Rest vs Encryption while Transmitting Data
- Scenarios where encryption would be considered "mandatory" versus "optional"

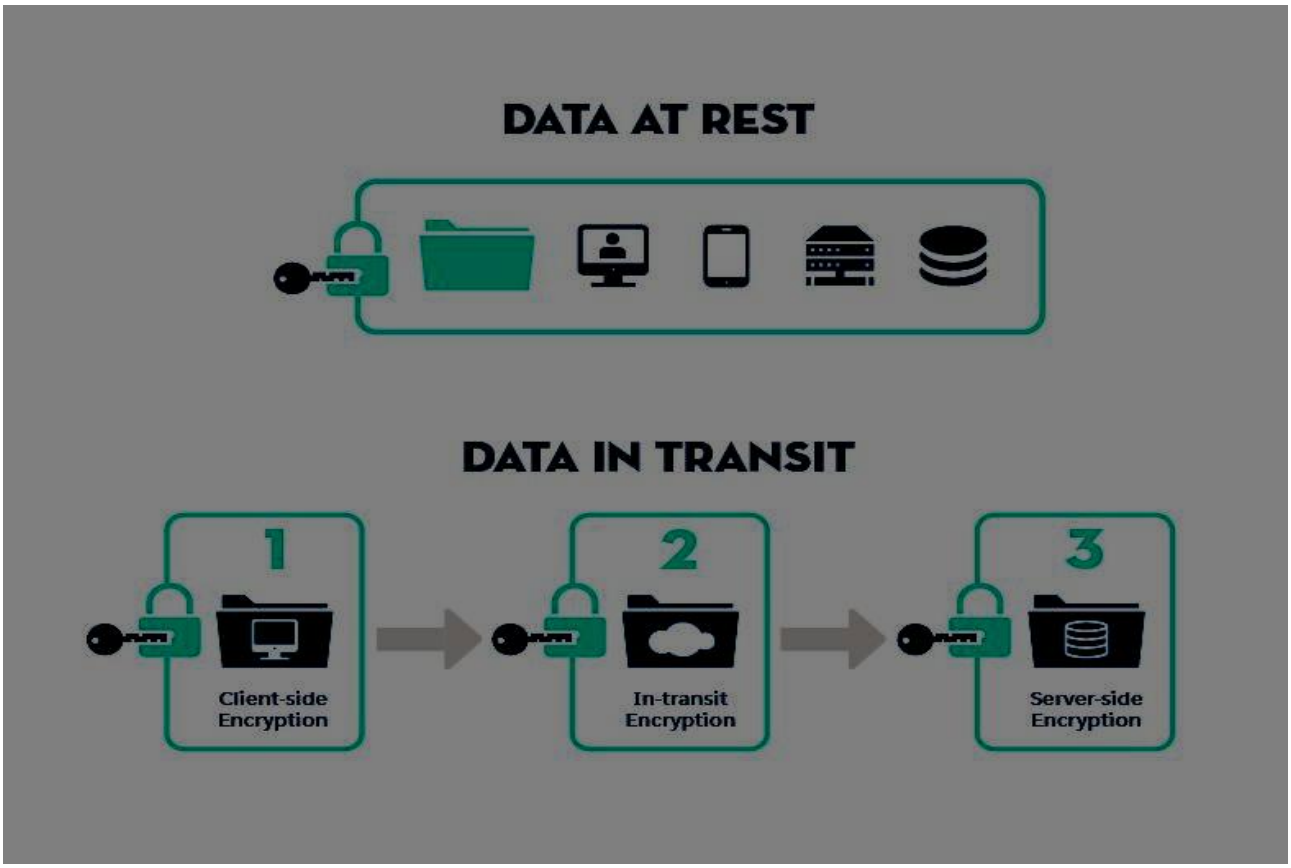
**Examples:**

- Emails
- Laptops

- Data Backups

**Common mistakes:**

- Assumes that all data must be encrypted
- Does not take into account actual risk




## 6. Backups, Availability & Resilience

**Covers:**

- Availability as a GDPR obligation
- Backup expectations
- Restore capability
- Ransomware considerations

**Examples:**

- Simple backup checklist (required)
- SME examples

**Common mistakes:**

- Assuming cloud = backup
- No restore testing

## 7. Training & Staff Awareness

**Covers:**

- Human Error as a Risk under GDPR.
- Expectations regarding training under GDPR.
- Awareness vs Formal Training Course Options.

**Examples:**

- Small Teams,
- Annual Refreshers

**Common mistakes:**

- One-off training only
- No record of training

## Common GDPR Security Myths & Misunderstandings

Examples:

- "GDPR requires encryption everywhere."
- "We need Cyber Essentials to comply with GDPR."
- "Antivirus software is sufficient for GDPR."
- "We are so small, we don't need to worry about GDPR."

Each myth clearly corrected.

## FAQs

- **Will the GDPR require me to encrypt my data?**

The GDPR does not stipulate that all data must be encrypted; however, encryption could be appropriate if your risks are significant (e.g., when handling sensitive data) and should be approached in a proportionate way.

- **Will antivirus software be enough for me to be GDPR compliant?**

No, you should include other controls alongside antivirus protection including access control measures and assess risks associated with your business.

- **Am I required to have Cyber Essentials in order to comply with the GDPR?**

Cyber Essentials is not mandatory with the GDPR; however, the ICO will view positively, as it is a measure of security adopted by an organisation when demonstrating compliance with data protection.

- **How quickly must I notify my customers about a breach?**

If your breach poses a risk to individuals, then you have 72 hours to notify the ICO. If your breach poses a high level of risk to individuals, then you must notify those individuals.

- **What evidence do I need to keep to prove my compliance?**

Maintain documents such as risk assessments, logs, policies and procedures—this is particularly easy for small businesses.

- **What is required with a small business' security under the GDPR?**

Ensure basic security controls (i.e., strong passwords) are proportionate to the data you hold and associated risk.

- **What are my responsibilities as a data controller?**

You are responsible for ensuring appropriate security controls are implemented and selecting secure data processors.

- **What does a risk-based approach mean?**

Your risk-based approach means assessing risks and costs related to the threat and avoiding unnecessary expense.

# About This Guide

The **Computer Support Centre** has developed this guide to educate and assist UK based IT managed services organisations to help Small to Medium Size Businesses (SMEs) protect their customers' personal information in the real world.

This document has been produced with the focus of being able to provide a simple, non-technical, plain English explanation of how IT Security obligations are enforced as a result of the UK GDPR legislation and to eliminate confusion regarding the significance of these obligations and to provide SMEs with the best available advice and resources concerning access control, device protection, incident response, backup, and supply chain management.

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



# Conclusion

The GDPR doesn't expect perfection or high tech costs - just that organisations proactively protect personal data through sound, logical, risk-based practices.

For most UK organisations, establishing a compliance posture that meets expectations of the GDPR regarding IT security will include establishing a strong foundation by focusing on core basic steps such as; managing access, securing devices, having reliable backups, being prepared for incidents, and training staff to understand their responsibilities for protecting data.

Organisations that focus on delivering practical security and enforced accountability can mitigate real risk, respond effectively to incidents, and demonstrate the responsible protection of data while not becoming over engineered or creating confusion.