FREE GUIDE

The 5 Most Common GDPR Mistakes, and How to Avoid Them

The five misunderstandings that catch small businesses out under Europe's data-protection law, each with a simple way to address it.

The General Data Protection Regulation (GDPR) is the European Union's law for handling people's personal data. Most small businesses don't fall short through bad intent. They fall short through a handful of avoidable misunderstandings. Here are the five that come up most often, and a simple way to address each.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Mistake 1: Assuming GDPR doesn't apply to you

"We're too small" and "we're not in Europe" are the most common misreadings, and the most expensive. GDPR applies to any organisation that handles the personal data of people in Europe, whatever the organisation's size and wherever it is based.

Avoid it: if you have European customers, website visitors, or staff, assume GDPR applies and work from there.

Mistake 2: Collecting personal data with no documented lawful basis

GDPR expects a specific, recorded legal reason for every kind of personal data you hold (Article 6): for example consent, a contract, a legal obligation, or legitimate interests. Many businesses collect first and never write down why.

Avoid it: list what you collect, and record the lawful basis for each type.

Mistake 3: Using everyday tools without a data processing agreement

Your email platform, analytics, customer database, and cloud storage all handle personal data on your behalf. Each one is expected to have a Data Processing Agreement in place (Article 28).

Avoid it: list every vendor that touches personal data, and confirm a signed agreement is in place with each.

Mistake 4: Keeping personal data "just in case"

Holding data with no retention limit sits poorly with the storage-limitation principle. Every record you keep is a record you must protect and could lose in a breach.

Avoid it: set a retention period for each type of data, and routinely delete what you no longer need.

Mistake 5: Having no plan for a breach or a data request

Two clocks catch businesses unprepared. A personal-data breach must usually be reported within 72 hours. A request from an individual to see their data must usually be answered within one month.

Avoid it: write a short, simple procedure for each, before you need it.

Where to go from here

The free GDPR self-assessment scores you across all five of these areas in about ten minutes. It runs entirely in your browser, so we never see your answers.

When you're ready to close the gaps with templates and workbooks built for small businesses, the GDPR Checklist toolkit lays it all out. Editions start at $49, one-time, with a 30-day money-back guarantee.

Take the free assessment: sylvanassurance.com/free/gdpr/

See the Full Edition: sylvanassurance.com/gdpr-checklist.html

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-gdpr-checklist