# The 5 General Data Protection Regulation (GDPR) Mistakes — and How to Avoid Them

GDPR Compliance Checklist

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-10-05

## Contents

**About This Guide** **2**

A plain-English guide for small business owners. GDPR is the European Union 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. 1. Assuming GDPR doesn't apply to you. "We're too small" and "we're not in Europe" are the most common (and most expensive) misreadings. 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. 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. 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 (Article 28). Avoid it: list every vendor that touches personal data, and confirm a signed agreement is in place with each. 4. Keeping personal data "just in case." Holding data with no retention limit sits poorly with the storage-limitation principle, and 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. 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, and 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.

Want to see where your business stands? The free GDPR self-assessment scores you across all five of these areas in about ten minutes. Provided by Sylvan Assurance, LLC as part of the GDPR Compliance Checklist. This is general, plain-English guidance, not legal advice. Compliance with the GDPR remains your responsibility; verify anything here against your own circumstances and, where needed, a qualified professional.

## About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience in data-protection and compliance work, translated into plain-language guidance for small business owners.

It provides **general guidance and recommended approaches**. It is **not** legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common compliance risk - and following it reduces exposure to common mistakes but **does not guarantee compliance and does not prevent enforcement**. Responsibility for your organisation's GDPR compliance remains with you.

For full terms, see the Terms of Use provided with the GDPR Compliance Checklist.

*Copyright 2026 Sylvan Assurance, LLC. Not for resale.*

*Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/*

### Where to go from here

Scan for the full toolkit that builds on this guide.
**sylvanassurance.com/go/toolkit-gdpr-checklist**

Scan for the companion book - the full story, in plain English.
**sylvanassurance.com/go/gdpr-compliance**