



Is Your Organisation Still GDPR Compliant? (The Cost of the “Set and Forget” Mistake)

Most organisations prepared their main GDPR documents several years ago. Privacy notices were published, internal policies were approved, and agreements with service providers were signed.

But businesses do not remain static.

Over the last few years, your organisation has likely evolved. New internal systems have been introduced. New service providers process your personal data. Marketing practices, recruitment processes, and customer communication channels have changed. **Most notably, employees may now use cloud platforms or artificial intelligence (AI) tools that didn't even exist when your original compliance documents were drafted.**

This creates a simple but critical question:

Do your data protection documents still reflect what your organisation actually does today?

GDPR Compliance is Not a One-Time Project

Having a privacy policy on your website does not automatically mean your organisation complies with the GDPR. True compliance means the organisation deeply understands:

- What personal data it processes and why it is genuinely needed;
- How long it is retained and who has access to it;
- Which external providers receive it and whether it is transferred internationally;
- How data subject requests and potential data breaches are handled.

The Golden Rule of GDPR: Your written documents must always correspond to your organisation's actual, day-to-day practices. If they don't, the documents themselves can become evidence of non-compliance.

When is a Data Protection Review Genuinely Useful?

A targeted review is highly recommended if your organisation:

- Has not updated its GDPR documentation for several years;
- Has introduced new IT systems, cloud services, or AI tools;
- Works with new international suppliers or SaaS providers;
- Has significantly changed its marketing, HR, or customer onboarding processes;
- Transfers personal data internationally (e.g., using overseas cloud tools or cross-border vendors);
- Has recently experienced a security incident or received complex data subject requests;
- Has never carried out a structured GDPR compliance review.

Note: A review is also appropriate before launching a new digital product, entering a new market, or making a significant pivot in operations.

Beyond “Check-the-Box” Legal Reports: What a Real Audit Provides

A useful audit should do much more than just identify missing documents. It should act as a business enabler, helping you understand:

1. Where your most significant legal and operational risks lie;
2. Which specific practices or documents require immediate attention;
3. What practical, cost-effective steps should be taken next.



The result should be a *clear, risk-prioritised action plan* rather than a purely theoretical, hundreds-of-pages-long legal report. Depending on your business, the audit can cover everything from cookie compliance and marketing automation to vendor agreements and cross-border data flows.

Does Every Organisation Need a Data Protection Officer (DPO)?

No. The GDPR requires a formal DPO only in specific circumstances.

However, even organisations exempt from this requirement benefit immensely from regular support from a data protection specialist. This ongoing support includes reviewing new projects and contracts, updating documentation, and helping the team respond swiftly to personal data breaches *before they become urgent, high-stakes crises.

How We Can Assist

Klauberg BALTICS advises organisations operating internationally on privacy, personal data protection, and GDPR compliance.

Our Data Protection Services include:

- **GDPR Health Checks:** A quick, practical audit to spot hidden risks in your current processes.
- **Documentation Updates:** Aligning your Contracts, Privacy Policies, Vendor Agreements, and Cookie management with current operations.
- **Handling Data Subject Requests:** Fully managing complex customer or employee requests.
- **Digital Privacy Training Platform:** Automated staff training via our subscription platform. Available in Latvian, English, with flexible localization into other languages upon request.
- **On-Demand data Protection Support:** reliable, text-and-call legal backing whenever you need it. We review new projects, evaluate tech vendors, and provide quick answers to your daily privacy questions without interfering with your regular processes.
- **External DPO Services:** Acting as your official designated Data Protection Officer to systematically manage and safeguard your privacy framework. This includes:
 - **Continuous Compliance Management:** Proactively monitoring your processes, identifying when documentation or practices need updates, and conducting regular employee trainings;

- **Privacy by Design & by Default:** Embedding data protection principles into the very architecture of your new products, services, or system integrations from day one;
- **Official Point of Contact:** Serving as your formal liaison for Data Protection Authorities during inspections, audits, and official inquiries;
- **Risk Assessments & Incident Response:*** Conducting Data Protection Impact Assessments (DPIAs), maintaining statutory logs, and leading the mitigation strategy in the event of a data breach.

Is it time to stress-test your privacy setup?

A data protection review can help determine whether your current documents still protect your business today – and what steps to take next.

Contact Our Team -

Meldra Emīlija Dzērve, meldra.dzerve@klauberg.legal for an Initial Assessment.

www.klauberg.legal SIA Zvērinātu advokātu birojs Klauberg
Elizabetes iela 85A-1
LV-1050 Rīga, Latvia