

GUIDE 2025/2026

GDPR guide for mid-sized companies

The General Data Protection Regulation, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is the GDPR? 3

1.1 The regulation in plain words 3

1.2 The seven principles of processing 3

1.3 Data subject rights — what people can ask of you 4

1.4 How it sits alongside other rules 4

2 Who needs a data protection officer? 6

3 The road to compliance — seven phases 8

4 What does GDPR compliance cost? 10

5 The ten most common mistakes 12

6 Readiness check: are you ready? 14

7 Glossary 16

8 Your next step 18

1 What is the GDPR?

1.1 The regulation in plain words

The **General Data Protection Regulation (GDPR)** is the central EU law protecting personal data — directly binding in every member state since **25 May 2018** . It governs how companies and public bodies may collect, process, store and pass on data about people.

Unlike a voluntary standard, the GDPR is **mandatory law**. Anyone processing personal data — and that means practically every company with staff, customers or suppliers — has to comply. In Germany it is supplemented by the Federal Data Protection Act (BDSG).

> **The core idea:** the GDPR does not ask “what data do you have?” but “can you show, for every processing activity, a legitimate purpose, a legal basis and appropriate safeguards?”

The sanctions bite: up to **€20 million or 4 % of worldwide annual turnover** (whichever is higher) for serious infringements. In recent years the German supervisory authorities have imposed fines in the millions — and the number of inspections keeps rising.

1.2 The seven principles of processing

Article 5 sets out seven principles that apply to every processing activity:

1. **Lawfulness, fairness and transparency** — a legal basis, plus clear communication to the people concerned.
2. **Purpose limitation** — process data only for specified, explicit and legitimate purposes.
3. **Data minimisation** — only as much data as you need, not “everything, just in case”.
4. **Accuracy** — data has to be factually correct and current, with corrections made promptly.
5. **Storage limitation** — do not keep data longer than necessary; a deletion plan is mandatory.
6. **Integrity and confidentiality** — appropriate technical and organisational measures.

7. **Accountability** — compliance with all the principles has to be documented and demonstrable.

> **An easy way to remember it:** the seventh principle is the operational anchor — without documented evidence (the processing record, impact assessments, the security measures, the logs) there is no GDPR compliance.

1.3 Data subject rights — what people can ask of you

The GDPR strengthens the rights of the people whose data you process. You have to be able to serve eight central rights within **one month** :

8	one month	72 hrs
data subject rights (Art. 15–22)	to reply (extendable to three)	to report a data breach

- **The right of access** (Art. 15) — which data is being processed?
- **The right to rectification** (Art. 16) — correcting inaccurate data.
- **The right to erasure, to be forgotten** (Art. 17) — removing data once the legal basis has gone.
- **The right to restriction** (Art. 18) — suspending the processing.
- **The right to data portability** (Art. 20) — receiving the data in machine-readable form.
- **The right to object** (Art. 21) — to certain processing activities.
- **The right not to be subject to automated decisions** (Art. 22).
- **The right to complain to the supervisory authority** (Art. 77).

1.4 How it sits alongside other rules

Rules	Focus	Relationship to the GDPR
GDPR	Personal data	The Europe-wide framework
BDSG	The German supplement	Uses the opening clauses
TTDSG / TDDDG	Telemedia and cookies	The specific law for the web

Rules	Focus	Relationship to the GDPR
ISO 27001	Information security	Covers most of the security measures
ISO 27701	Privacy information management	An ISO standard aligned to the GDPR

Worth knowing: ISO 27001 and 27701 do not replace the GDPR — but they give you a dependable management system that covers 70 to 80 % of its technical and organisational requirements.

2 Who needs a data protection officer?

The GDPR distinguishes between cases where appointing a data protection officer is required and cases where it is merely advisable. The German BDSG lowers the threshold considerably.

A. Where an officer is required by law

Under the GDPR (Art. 37)

- Your core activity involves regular and systematic monitoring of people on a large scale — online tracking or video surveillance, for example.
- Your core activity involves large-scale processing of special categories: health data, biometric data, data on religious belief and so on.
- Public authorities and bodies.

Under § 38 BDSG (the German supplement)

- **From 20 people** routinely engaged in the automated processing of personal data.
- Where a data protection impact assessment is required under Art. 35.
- Where data is processed commercially for transfer, anonymised transfer, or for market and opinion research.

> **The practical threshold in Germany:** once 20 staff handle customer data, personnel data or websites with tracking, an officer becomes mandatory. In practice that covers almost every company of that size.

B. Internal or external officer?

The GDPR allows either:

Criterion	Internal officer	External officer
Knowledge	Knows the company well	Broad professional expertise
Cost	Salary plus training	A fixed monthly fee (from €249)
Liability	May conflict with their other role in the company	Independence assured

Criterion	Internal officer	External officer
Protection against dismissal	Enhanced (§ 38(2) BDSG)	By contract, more flexible
Availability	Only on site	Phone, e-mail, video, on site

For a mid-sized company the **external officer** is usually the more economical and legally safer choice — you get the expertise without the staffing risk and without conflicts of interest.

C. What the officer does (Art. 39)

- Informing and advising the controller and the staff
- Monitoring compliance with the GDPR and with internal privacy policies
- Advising on data protection impact assessments
- Cooperating with the supervisory authority
- Acting as the point of contact for data subject requests
- Training the staff

> *A real example: an e-commerce company with 35 staff handles customer and employee data, uses tracking tools and sends newsletters. Under the BDSG it has to appoint an officer. Its decision: an external officer at €249 a month — €2,988 a year, less than a single impact assessment bought from another consultancy.*

3 The road to compliance — seven phases

GDPR compliance is an ongoing process, not a one-off project. To build it up in a structured way, allow **two to six months**, depending on your size and on what you have already done.

1 **Take stock and analyse the gaps**

Which data is processed where, why and for how long? Go through every process: HR, sales, marketing, IT, providers. The result is a list of all processing activities. Two to three weeks.

2 **The record of processing**

A structured document under Art. 30. For each activity: purpose, legal basis, categories of data and of people, recipients, retention periods and security measures. Mandatory from 250 staff, and in practice advisable for everyone. Three to five weeks.

3 **Settle the legal bases and the agreements**

Set the legal basis for each activity under Art. 6 — consent, contract, legitimate interest and so on. Sign or refresh data processing agreements with every provider: cloud, HR software, marketing tools. Three to four weeks.

4 **Technical and organisational measures**

The measures required by Art. 32: access control, encryption, backup, a permissions model, logging — and the document that records them. Four to six weeks.

5 **A process for data subject rights**

Standard processes for the eight rights. Who answers within the month? How do we recognise a request? How do we record what we did? Plus the breach notification process and its 72-hour deadline. Two to three weeks.

6 **Training and awareness**

A basic course for everyone, with more depth for HR, marketing, sales and IT. Record attendance and refresh it at least every two years. One to two weeks to begin with.

7 **Appoint the officer and set up privacy management**

> Appoint an internal or external officer and notify the supervisory authority. Set an annual plan for the officer's audit, the training cycle, the review of security measures and contract updates. One to two weeks.

Tip: Start with the processing record and a review of your processor agreements. Those are the two things supervisory authorities look at most often — getting them right cuts the risk of a fine considerably.

4 What does GDPR compliance cost?

GDPR costs fall into **the one-off build** and **the running costs** (mainly the officer's fee). Here are realistic ranges for a mid-sized company:

Company size	One-off build*	Timeframe	Internal effort
1–9 staff	**€3,900–5,500**	2–4 months	4–8 hrs/week
10–49 staff	**€5,500–8,000**	3–5 months	6–10 hrs/week
50–249 staff	**€8,000–12,000**	4–6 months	8–14 hrs/week
250–999 staff	**€12,000–18,000**	5–8 months	12–20 hrs/week
1,000+ staff	**€18,000–26,000**	7–10 months	16–28 hrs/week

* Includes consulting, producing the processing record and the security documentation, the set of processor agreements, training material and appointing the officer. **Excludes the** external officer.

Running costs — the external officer

The external data protection officer is the largest running cost. Monthly fees vary with complexity:

- **Basic:** from €249 a month, including a basic helpline, the annual audit and handling data subject requests.
- **Premium:** €400–800 a month where advice is needed often or the data landscape is complex.
- **On top**: impact assessments (€890–2,490 per case) and emergency help after a breach.

What drives the cost?

- **How many processing activities you have:** the more systems, tools and providers, the bigger the processing record.
- **Your industry:** health, marketing and HR-heavy businesses face more work.
- **Where you start:** existing documentation (ISO 27001, quality management) cuts the cost by 30 to 40 %.
- **How many staff you have:** more staff means more training, more HR processes and more agreements.

In the interest of transparency: a data breach can bring further costs: forensics, legal advice, the reporting process. A good officer is protection — the investment usually pays for itself after the first serious incident.

5 The ten most common mistakes

From our work as data protection officers, we know the usual stumbling blocks in mid-sized companies:

1. **No complete processing record**
   The record is required by Art. 30. If it is missing or has holes, it is the first thing any inspection picks up — and the most common ground for a fine.

2. **Missing or outdated processor agreements**
   Every processor — cloud, HR tool, mailing provider — needs an agreement under Art. 28. Many contracts from 2018 are legally out of date by now.

3. **No deletion plan**
   Art. 5(1)(e) requires storage limitation. Without a documented plan with retention periods per category of data, there is no evidence.

4. **Ignoring third-country transfers**
   Using US tools without an arrangement that satisfies Schrems II — even under the EU-US Data Privacy Framework there is still risk if the assessment is sloppy.

5. **Consent that will not hold up**
   Marketing opt-in has to be freely given, informed, specific and demonstrable. Many consent banners are none of those.

6. **No structure for data subject requests**
   An access request has to be answered within one month. Without a process and a template the deadline slips — a direct ground for a complaint and a fine.

7. **No impact assessment**
   For high-risk processing — video surveillance, tracking, AI systems — an impact assessment is mandatory. Skip it and the whole activity becomes challengeable.

8 **No officer appointed — or appointed but not notified**

Despite the BDSG threshold, many companies have no officer. Or they have one but never notified the supervisory authority — which is an offence in itself.

9 **No staff training**

Around 60 % of privacy incidents come from human error. Without regular training the risk stays high — and the officer cannot meet their duty to inform.

10 **Reporting a breach too late**

Art. 33 requires notification within 72 hours. Reporting later risks a larger fine AND damage to reputation — authorities come down hard on late reports.

6 Readiness check: are you ready?

Answer the following ten questions honestly, yes or no. The result shows your GDPR maturity:

1. **Do you have an up-to-date record of processing activities?**
   Every activity documented — purpose, legal basis, retention period, security measures.
2. **Have you appointed a data protection officer and notified the authority?**
   Internal or external — and registered with the state data protection authority.
3. **Do you have agreements with every provider that processes data?**
   Cloud, HR tools, mailing, accounting, external IT.
4. **Is there a documented set of security measures under Art. 32?**
   Access control, encryption, backup, a permissions model.
5. **Do you have a documented deletion plan with retention periods?**
   Per category of data: when to delete, and the exceptions where you must keep it.
6. **Is there a process for data subject requests within the one-month deadline?**
   Who receives, answers and records them? Is there a standard template?
7. **Is there a breach notification process for the 72-hour deadline?**
   An escalation chain, a notification template, and a decision on whether it is reportable.
8. **Have you carried out an impact assessment for high-risk processing?**
   Video surveillance, tracking, profiling, AI systems, sensitive data.
9. **Have your staff had GDPR training in the last twelve months?**
   With attendance recorded and extra depth by role.
10. **Is your website privacy policy current and legally sound?**
    A compliant cookie banner, every tool named, the rights explained.

Your yes answers	Assessment	Recommendation
0–3 × yes	**Acutely exposed**	An inspection or a breach would bring a high risk of a fine. Start building now. Three to five months.

Your yes answers	Assessment	Recommendation
4–6 × yes	**Partly prepared**	Focus on the gaps — the processing record, the agreements, the deletion plan. Two to three months to finish.
7–10 × yes	**A good basis**	Fine-tuning, regular audits, keeping it running. No urgent gaps.

Whatever your result: **GDPR compliance is a continuous task**, not a box to tick once. A short annual review and adjustment avoids most of the risk.

7 Glossary

The key GDPR terms, explained plainly:

GDPR

General Data Protection Regulation (EU 2016/679) — binding in every EU member state since May 2018.

BDSG

The German Federal Data Protection Act — the national supplement to the GDPR, setting the officer threshold at 20 people, for example.

Personal data

Any information about an identified or identifiable natural person (Art. 4(1)).

Controller

Whoever determines the purposes and means of processing — usually the company itself.

Processor

An external provider processing data on the controller's behalf — cloud, SaaS, service providers.

VVT

The record of processing activities (Art. 30) — structured documentation of every activity involving personal data.

AVV

Data processing agreement (Art. 28) — the mandatory contract with every processor.

TOM

Technical and organisational measures (Art. 32) — the safeguards against unauthorised access and the like.

DSFA

Data protection impact assessment (Art. 35) — a risk analysis before introducing high-risk processing.

DSB

Data protection officer — a mandatory role in certain companies (§ 38 BDSG, Art. 37 GDPR).

Data subject rights

The eight rights of the people whose data is processed (Art. 15–22 and 77).

Data breach

A breach of the protection of personal data (Art. 33, 34) — reportable to the supervisory authority within 72 hours.

Special categories

Data under Art. 9: health, biometrics, religion, politics, sexual orientation and so on. Stricter rules apply.

Third-country transfer

Transferring data outside the EU or EEA — permitted only with an adequacy decision, standard contractual clauses or binding corporate rules.

Accountability

Art. 5(2) — the controller has to be able to demonstrate compliance with all the principles.

8 Your next step

You have read this guide — that is the first step already. Tackling GDPR compliance in a structured way protects you from fines, strengthens your customers' trust, and is the basis for many further compliance requirements: NIS-2, ISO 27001, TISAX.

A free first conversation

In 30 minutes, with no obligation, we work out together:

- ✓ Where do you stand on the GDPR today?
- ✓ Do you need an external data protection officer?
- ✓ Which gaps come first?
- ✓ What budget and timeframe are realistic?

No sales pitch, no pressure — just an honest assessment.

> **The quick GDPR check**
> At **iso-easy.de** you will find our free GDPR check. In a few minutes you get a first view of where you stand and what needs doing.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and information security we support mid-sized companies in implementing the GDPR, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.