2026 EDITION

The GDPR Complete Guide

From Regulation to Reality — everything European small and medium businesses need to know, updated with the latest enforcement data, AI guidance and practical templates.

GDPRGard

gdprgard.eu · AI Compliance Suite for European SMBs

ABOUT THIS GUIDE

Who this is for

This guide is written for founders, managers and operations teams at European small and medium businesses — people who need to get GDPR right without a legal department. Every chapter translates the regulation into plain language, connects it to a concrete obligation, and tells you what to actually do about it.

The 2026 edition adds updated enforcement statistics, the latest case studies, expanded coverage of AI and the EU AI Act, and notes on the European Commission's Digital Omnibus proposals affecting GDPR record-keeping for smaller companies.

Important: *this guide is educational material, not legal advice. It is a strong starting point — but for high-stakes decisions, have a qualified lawyer or data protection officer review your specific situation. GDPRGard's Expert plan exists for exactly that.*

CONTENTS

What's inside

APPENDICES

A. Glossary: 30 terms in plain language

B. Your first 30 days, week by week

C. Supervisory authorities: who regulates you

D. The ten questions a regulator asks first

PART I

The Regulation

Where GDPR came from, who it applies to, and the vocabulary you need.

CHAPTER 1

Origins, scope & definitions

The General Data Protection Regulation (EU) 2016/679 took effect on 25 May 2018, replacing the 1995 Data Protection Directive. Unlike a directive, a regulation applies directly in every member state — the same core rules from Lisbon to Helsinki.

Territorial scope (Article 3)

GDPR applies to you if you are established in the EU/EEA and process personal data — regardless of where the processing happens — or if you are established elsewhere but offer goods or services to people in the EU or monitor their behaviour. A US webshop shipping to Germany and a Croatian café with a customer newsletter are both in scope.

The vocabulary that matters

- **Personal data** — any information relating to an identified or identifiable person: names, emails, IP addresses, location data, customer IDs, photos.
- **Processing** — practically anything you do with personal data: collecting, storing, reading, sharing, deleting.
- **Controller** — the party deciding *why* and *how* data is processed. If it's your customer list, that's you.
- **Processor** — a party processing on the controller's behalf: your email platform, cloud host, payroll bureau.
- **Special categories (Art. 9)** — health, biometrics, religion, politics, sexuality, trade-union membership. Processing these needs a separate, stronger justification.

There is no small-business exemption from GDPR itself. Article 30(5) softens record-keeping for organisations under 250 employees in narrow cases, but the core obligations apply from your first customer record.

CHAPTER 2

The six principles (Article 5)

Article 5 is the spine of the regulation. Every specific rule in GDPR traces back to one of these principles — and regulators cite Article 5 in most fines.

- **1. Lawfulness, fairness, transparency** — every processing operation needs a legal basis, and people must be able to understand what you do with their data.
- **2. Purpose limitation** — collect data for a specific, stated purpose; don't quietly reuse it for something else.
- **3. Data minimisation** — collect what you need, nothing more. A newsletter needs an email address, not a birth date.
- **4. Accuracy** — keep data correct and up to date; correct or delete inaccurate data promptly.
- **5. Storage limitation** — keep data only as long as needed for the purpose. Define retention periods and enforce them.
- **6. Integrity and confidentiality** — protect data with appropriate security: encryption, access control, backups.

The seventh obligation: accountability

Article 5(2) adds the principle that changes everything for SMBs: you must be able to **demonstrate** compliance. It is not enough to behave well — you need records, policies and documented decisions. That is why the Records of Processing Activities, privacy notices and DPIAs in Part V matter: they are your evidence.

CHAPTER 3

Lawful bases (Articles 6–10)

Every processing operation needs exactly one lawful basis from Article 6, chosen *before* you start processing. The six options:

- **Consent (6(1)(a))** — a freely given, specific, informed, unambiguous opt-in. Pre-ticked boxes and bundled consent are invalid. People must be able to withdraw as easily as they gave it.
- **Contract (6(1)(b))** — processing needed to deliver what the person asked for: shipping address for an order, email for a receipt.
- **Legal obligation (6(1)(c))** — tax record retention, employment law filings.
- **Vital interests (6(1)(d))** — life-or-death situations; rarely relevant to businesses.
- **Public task (6(1)(e))** — mostly for public authorities.
- **Legitimate interest (6(1)(f))** — the flexible basis: fraud prevention, direct marketing to existing customers, IT security. Requires a documented three-part balancing test: identify the interest, show necessity, and weigh it against the person's rights.

Choosing well

The most common SMB mistake is defaulting to consent for everything. Consent is fragile — it can be withdrawn at any moment and must be provable. If the processing is genuinely needed to deliver your service, contract is the better basis; if it's a reasonable business need, run the legitimate-interest test and document it.

Special categories (Article 9) need an additional condition on top of the Article 6 basis — most commonly explicit consent or employment-law necessity. Criminal-offence data (Article 10) is stricter still.

PART II

Rights & Obligations

What people can demand from you, and what the regulation demands of you.

CHAPTER 4

Data subject rights (Articles 12–22)

GDPR gives every person eight enforceable rights over their data. You must respond to a request **within one month** (extendable by two months for complex cases — but you must say so within the first month), free of charge in almost all cases.

- **Information (Arts. 13–14)** — people must be told what you collect and why, at the moment of collection. Your privacy notice does this job.
- **Access (Art. 15)** — a copy of everything you hold about them, plus the purposes, recipients and retention periods.
- **Rectification (Art. 16)** — correction of inaccurate data.
- **Erasure (Art. 17)** — the 'right to be forgotten' where data is no longer needed, consent is withdrawn, or processing was unlawful. Not absolute — legal retention duties override it.
- **Restriction (Art. 18)** — 'freeze' processing while a dispute is resolved.
- **Portability (Art. 20)** — data provided by the person, in a machine-readable format, for consent- or contract-based processing.
- **Objection (Art. 21)** — an absolute right to stop direct marketing; a qualified right against legitimate-interest processing.
- **Automated decisions (Art. 22)** — protection against purely automated decisions with legal or similarly significant effects — increasingly relevant as SMBs adopt AI (see Chapter 11).

Handling requests without drama

Create one intake channel (a dedicated email address works), verify identity proportionately, log every request and its outcome, and prepare response templates in advance. Most SMB failures here are process failures — the one-month clock runs out because nobody owned the request.

CHAPTER 5

Controller & processor duties

Your obligations by design (Articles 24–25)

Controllers must implement 'appropriate technical and organisational measures' — proportionate to your risk, which is what makes GDPR workable for a five-person company. Data protection by design and by default (Article 25) means privacy is built into new products and processes from the start: the signup form that collects only what it needs, the CRM configured to auto-delete stale leads.

The Records of Processing Activities (Article 30)

Your RoPA is a structured inventory of every processing activity: purpose, categories of data and people, recipients, transfers, retention, security measures. Regulators routinely request it within days of first contact — it is the single document that proves you know what you're doing with data. Part V shows how to build one in an afternoon.

Processors and contracts (Article 28)

Every processor you use — email platform, host, accountant's software — must be bound by a Data Processing Agreement covering the Article 28(3) mandatory clauses: documented instructions, confidentiality, security, sub-processor rules, deletion at contract end, and audit rights. Most reputable SaaS vendors publish a signable DPA; your job is to actually check it exists, and keep a vendor register (which doubles as the transfer map for Chapter 10).

Do you need a DPO (Articles 37–39)?

Most SMBs do not. A Data Protection Officer is mandatory only for public authorities, or where core activities involve large-scale regular monitoring or large-scale special-category processing. Appointing a voluntary DPO binds you to the full DPO framework — often the smarter move is a named internal privacy lead plus external advice when needed.

CHAPTER 6

Breach notification (Articles 33–34)

A personal data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data — a hacked mailbox, a laptop left on a train, an email sent to the wrong recipient list, ransomware.

The 72-hour clock (Article 33)

You must notify your supervisory authority **within 72 hours of becoming aware** of a breach, unless it is unlikely to result in risk to individuals. The clock starts when you have a reasonable degree of certainty a breach occurred — weekends included. Late notification is itself a fineable offence, separate from the breach.

Your notification must describe the nature of the breach, categories and approximate numbers of people and records affected, likely consequences, measures taken, and a contact point. You may notify in phases if you don't have everything within 72 hours — notify first, complete later.

Telling the people affected (Article 34)

Where the breach is likely to result in *high* risk — identity theft, fraud, exposure of sensitive data — you must also inform the affected individuals without undue delay, in clear language, with concrete advice on protecting themselves.

Every breach — even ones you don't have to report — must be documented internally in a breach register: facts, effects, remedial action. Chapter 14 provides the complete response template. GDPRGard's BreachNotify tool assesses reportability and drafts both notifications inside the deadline.

PART III

Enforcement & Penalties

What non-compliance actually costs, and what the fines teach.

CHAPTER 7

Fines & penalties (Articles 83–84)

GDPR fines come in two tiers. The lower tier — up to **€10 million or 2% of global annual turnover**, whichever is higher — covers failures like missing records, ignoring breach notification, or skipping a required DPIA. The upper tier — up to **€20 million or 4% of turnover** — covers violations of the principles, lawful bases, data subject rights and international transfer rules.

How authorities set the amount

Article 83(2) lists the factors: nature and duration of the infringement, number of people affected, intent or negligence, mitigation efforts, previous infringements, cooperation, data categories involved, and how the authority learned of it. The EDPB's 2023 fining guidelines harmonised the methodology across the EU: a starting amount based on seriousness and turnover, adjusted for those factors.

Beyond fines

Authorities can also warn, reprimand, order compliance within a deadline, restrict or **ban processing outright** — which for a data-driven business can hurt more than the fine — and order suspension of data flows to third countries. People affected can claim compensation (Article 82), including for non-material damage, and collective actions are growing across member states.

For SMBs the real exposure is rarely a headline mega-fine. It is the €5,000–€100,000 penalty for a missing privacy notice, an ignored access request or an unreported breach — combined with legal costs, remediation and reputational damage.

CHAPTER 8

Enforcement in numbers

Seven years in, the enforcement picture is clear: cumulative GDPR fines passed **€6.1 billion** across more than 2,600 published penalties, and the pace is accelerating rather than slowing.

What the statistics show

- **Ireland leads by amount** — the Irish DPC, supervising Big Tech's EU headquarters, has issued the largest total (over €3.5B), including the record €1.2B Meta transfer fine.
- **Spain leads by volume** — hundreds of smaller fines, showing that high-frequency enforcement against ordinary businesses is the norm in some markets.
- **The most-cited articles** — Article 5 (principles), Article 6 (lawful basis) and Article 32 (security) appear in the majority of decisions. Fines rarely punish exotic failures; they punish basics.
- **SMBs are fined too** — restaurants using CCTV unlawfully, retailers ignoring access requests, clinics emailing patient data unencrypted. Small penalties, but existential at small scale.

The trend into 2026

Three themes dominate current enforcement: (1) cookies and consent-or-pay models, with coordinated EDPB attention; (2) AI training data and automated decision-making, following the EDPB's 2024 opinion on AI models; and (3) cross-border transfers. At the same time, the Commission's Digital Omnibus package (proposed November 2025) aims to simplify record-keeping duties for smaller companies — a proposal still moving through the legislative process in 2026, and no reason to pause compliance work: the principles and rights it would leave untouched are exactly where fines concentrate.

CHAPTER 9

Case studies: Meta, LinkedIn, Uber, TikTok

Meta — €1.2 billion (2023): transfers

The largest GDPR fine ever, from the Irish DPC after EDPB intervention, for transferring European user data to the US without adequate safeguards after Schrems II. **Lesson:** transfer compliance is not paperwork — know where your data physically goes, including via your vendors.

LinkedIn — €310 million (2024): lawful basis

The Irish DPC found LinkedIn's behavioural advertising could not rest on contract or legitimate interest as claimed; consent was required. **Lesson:** choosing a convenient lawful basis rather than a correct one is itself the violation. Document why your basis fits before processing starts.

Uber — €290 million (2024): transfers again

The Dutch AP fined Uber for moving driver data — including documents and criminal-record data — to US servers for two years without valid transfer tools after it stopped using Standard Contractual Clauses. **Lesson:** transfer safeguards must be continuous. When a mechanism lapses, the processing must stop until a new one is in place.

TikTok — €345M (2023) and €530M (2025): children & transfers

First fined for children's default-public settings and dark patterns, then €530M for transfers of European data accessible from China and transparency failures. **Lesson:** defaults are compliance decisions (Article 25), and 'remote access from' a third country *is* a transfer.

Four giant fines, four SMB-sized morals: map your data flows, justify your lawful basis in writing, keep transfer safeguards alive, and make the private option the default.

PART IV

Advanced Topics

Transfers, artificial intelligence, and the new AI Act — where GDPR is heading.

CHAPTER 10

International transfers

Chapter V of GDPR restricts moving personal data outside the EU/EEA. 'Transfer' is broad: hosting on a US cloud, a support team in India viewing your CRM, an analytics script sending data to American servers.

The three lawful routes

- **Adequacy decisions (Art. 45)** — the Commission has declared some countries adequate: the UK, Switzerland, Japan, South Korea, Canada (commercial), and the US — but only for companies certified under the EU-US Data Privacy Framework. Check your vendor's certification, don't assume it.
- **Appropriate safeguards (Art. 46)** — most commonly Standard Contractual Clauses (the 2021 modules), plus a documented Transfer Impact Assessment showing the destination country's laws don't undermine the clauses in practice.
- **Derogations (Art. 49)** — explicit consent or contractual necessity for occasional, non-repetitive transfers. Not a foundation for routine operations.

What an SMB should actually do

Inventory your vendors (your Article 30 record already lists them), mark where each stores and accesses data, and for each non-EU destination note the mechanism: DPF certification, SCCs + TIA, or adequacy. Re-check annually — as Uber learned, a safeguard that quietly lapsed is a €290M problem at scale, and a real problem at any scale.

CHAPTER 11

GDPR & AI in 2026

AI does not get a GDPR exemption. If personal data goes into a model — for training, fine-tuning or prompts — every principle from Part I applies. Three questions matter for an SMB using AI tools:

1. What goes in?

Feeding customer emails, CVs or health notes into an AI tool is processing. Choose tools that don't retain or train on your inputs (or offer that guarantee contractually), minimise what you paste, and cover AI vendors in your DPAs and vendor register like any other processor. Anonymise where the task allows it.

2. Who decides?

Article 22 restricts purely automated decisions with significant effects — loan approvals, CV rejections, account terminations. The safe pattern is meaningful human review: a person with authority and information to overrule the machine, not a rubber stamp. Document where AI-assisted decisions happen in your business and where the human sits in each.

3. Can you explain it?

Transparency obligations extend to AI: privacy notices must say that AI is used, for what, and with what logic in broad terms. The EDPB's 2024 opinion on AI models confirmed regulators' expectations: a documented lawful basis (usually a carefully reasoned legitimate interest) for training, and effective data subject rights even when data is inside a model.

A DPIA is required for most substantial AI deployments touching personal data — systematic evaluation, large-scale processing or new technology all trigger Article 35. Chapter 15's template covers it.

CHAPTER 12

The EU AI Act intersection

The AI Act (Regulation 2024/1689) entered into force in August 2024 and applies in stages: prohibitions and AI-literacy duties since February 2025, general-purpose AI rules since August 2025, and the bulk of high-risk obligations arriving August 2026. It regulates *systems* by risk level, while GDPR regulates *personal data* — most business AI use touches both.

What SMBs actually need to know

- **Prohibited practices** — social scoring, emotion recognition at work, manipulative techniques. Simply don't.
- **High-risk uses** — AI in recruitment, credit, essential services. If you *deploy* such systems (even bought, not built), you owe human oversight, input quality, logging and vendor-instruction duties from August 2026.
- **Limited-risk transparency** — chatbots must be identifiable as AI; synthetic media must be labelled.
- **AI literacy (Art. 4)** — everyone providing or deploying AI must ensure staff using it are adequately trained. This applies to SMBs now — a short internal training and usage policy covers it.

One compliance programme, not two

The overlaps are your friend: the AI Act's risk management pairs with GDPR's DPIA; its human-oversight duty operationalises Article 22; its logging supports accountability. Run them as one workstream. GDPRGard's free AI Human Oversight Checklist maps the shared controls.

PART V

Practical Compliance

The checklist and templates that turn the previous 12 chapters into an afternoon of work.

CHAPTER 13

The 20-point SMB checklist

Work through these in order. Points 1–7 are the foundation; 8–14 are your documents; 15–20 are operations. Each maps to the chapter in brackets.

- 1. List every place personal data lives: CRM, inbox, payroll, analytics, backups. (Ch. 1)
- 2. Build your Article 30 RoPA from that list — purpose, data, recipients, retention per activity. (Ch. 5)
- 3. Assign one named owner for privacy. (Ch. 5)
- 4. Choose and record a lawful basis for each activity. (Ch. 3)
- 5. Run and document the balancing test for every legitimate-interest use. (Ch. 3)
- 6. Identify special-category data; add its extra condition or stop collecting it. (Ch. 3)
- 7. Map international transfers and their safeguards. (Ch. 10)
- 8. Publish a plain-language privacy notice covering Articles 13–14. (Ch. 4)
- 9. Publish a cookie policy and a banner where consent is real: reject as easy as accept. (Ch. 2)
- 10. Sign DPAs with every processor; keep a vendor register. (Ch. 5)
- 11. Set retention periods per data category — and automate deletion where possible. (Ch. 2)
- 12. Create your breach register and response plan. (Ch. 6, 14)
- 13. Prepare data subject request templates and an intake channel. (Ch. 4)
- 14. Screen new projects for DPIA triggers; run DPIAs where required. (Ch. 15)
- 15. Enable encryption at rest and in transit, MFA, and least-privilege access. (Ch. 2)
- 16. Train every employee briefly, twice a year — include AI usage rules. (Ch. 11, 12)
- 17. Test your breach plan with a one-hour tabletop drill. (Ch. 6)
- 18. Answer test: could you fulfil an access request within a month? Fix what blocked you. (Ch. 4)
- 19. Review vendors, transfers and retention annually; log the review. (Ch. 5, 10)
- 20. Keep evidence of all of the above in one folder — accountability is demonstrability. (Ch. 2)

Score yourself honestly: 0–10 points done means start at point 1 today; 11–16 means close the documentation gaps; 17+ means you're audit-ready — keep the annual rhythm. GDPRGard's free compliance checker automates this scoring.

CHAPTER 14

The 72-hour breach response template

Copy this into your incident plan. Times are from the moment of awareness (T0).

Hour 0–4 — Contain and convene

- Isolate affected systems; preserve logs and evidence — contain, don't destroy.
- Convene your response group: privacy lead, IT, management. One person leads; one person writes everything down with timestamps.

Hour 4–24 — Assess

- Establish: what data, whose, how many, since when, still ongoing?
- Risk-assess for individuals: identity theft, fraud, discrimination, distress.
- Decision point: notifiable? If risk is likely — notify. If genuinely unlikely — document exactly why not in the breach register.

Hour 24–72 — Notify

- Submit the Article 33 notification to your supervisory authority: nature of the breach, categories and approximate numbers, likely consequences, measures taken, contact point. Use phased notification if facts are incomplete — never wait for perfection past 72 hours.
- If high risk: draft the Article 34 notice to affected people in plain language with concrete protective steps, and send without undue delay.

After — Close the loop

- Complete the breach register entry: facts, effects, remediation.
- Run a post-incident review within two weeks; fix the root cause; update this plan with what you learned.

GDPRGard's BreachNotify walks through this assessment interactively and generates both notifications — with emergency support when the clock is running.

CHAPTER 15

Privacy policy & DPIA templates

Privacy notice — the ten sections that make it compliant

A compliant notice under Articles 13–14 answers, in plain language: (1) who you are and how to reach you; (2) what data you collect; (3) why — purpose by purpose; (4) the lawful basis for each purpose; (5) who receives it, including processors; (6) transfers outside the EU and their safeguards; (7) how long you keep it; (8) the eight rights and how to exercise them; (9) the right to complain to a supervisory authority; (10) whether automated decision-making is used, with meaningful information about the logic. One purpose per row of a simple table beats ten pages of legalese — for you and for the regulator.

DPIA — when and how (Article 35)

A Data Protection Impact Assessment is mandatory where processing is 'likely to result in high risk': systematic profiling with significant effects, large-scale special-category processing, systematic public monitoring — and, per authority blacklists, most new-technology deployments such as substantial AI systems. When in doubt, run one: it is the cheapest insurance in this book.

The template has five parts:

- **1. Description** — the processing, its purposes, data flows, and a diagram if it helps.
- **2. Necessity & proportionality** — why this data, this scope, this retention; lawful basis; minimisation choices.
- **3. Risk assessment** — for individuals, not the business: likelihood × severity of illegitimate access, unwanted modification, disappearance of data.
- **4. Mitigations** — the measures reducing each risk: encryption, access control, human oversight, retention cuts, vendor terms.
- **5. Sign-off** — residual risk accepted by a named owner and date; DPO advice if you have one; consultation with the authority if high residual risk remains.

Generate both documents in minutes with GDPRGard's privacy policy generator and DPIA tooling — tailored to your jurisdiction and in your language — then have them reviewed as Chapter 1 advises.

APPENDIX A

Glossary: 30 terms in plain language

- **Adequacy decision** — The Commission's ruling that a non-EU country protects data well enough for free transfers.
- **Anonymisation** — Irreversibly removing the link to a person. Truly anonymous data is outside GDPR; pseudonymised data is not.
- **Article 30 record / RoPA** — Your structured inventory of every processing activity — the first document a regulator asks for.
- **Automated decision-making** — A decision made by a machine without meaningful human involvement (Article 22).
- **Consent** — A freely given, specific, informed, unambiguous opt-in — as easy to withdraw as to give.
- **Controller** — The party that decides why and how personal data is processed.
- **Cookie wall** — Blocking access unless tracking is accepted. Generally invalid consent.
- **Data Privacy Framework (DPF)** — The EU–US adequacy arrangement; valid only for US companies certified under it.
- **Data subject** — The living person the data is about — customer, employee, visitor.
- **DPA (agreement)** — Data Processing Agreement — the Article 28 contract binding every processor you use.
- **DPIA** — Data Protection Impact Assessment — the structured risk analysis required for high-risk processing (Article 35).
- **DPO** — Data Protection Officer — mandatory only for public bodies and large-scale monitoring or special-category processing.
- **EDPB** — European Data Protection Board — the EU body that coordinates supervisory authorities and issues guidance.
- **Erasure ('right to be forgotten')** — The right to have data deleted when it is no longer lawfully needed (Article 17).
- **Joint controllers** — Two or more parties deciding purposes together — requires an arrangement allocating duties (Article 26).
- **Lawful basis** — One of the six Article 6 justifications every processing operation must have before it starts.
- **Legitimate interest** — The flexible lawful basis requiring a documented three-part balancing test.
- **Personal data** — Any information relating to an identified or identifiable person — including IP addresses and IDs.
- **Personal data breach** — Any incident leading to accidental or unlawful loss, alteration, disclosure of, or access to personal data.

- **Privacy by design / by default** — Building data protection into products from the start, with the most private settings as default (Article 25).
- **Processing** — Anything done with personal data: collecting, storing, reading, sharing, deleting.
- **Processor** — A party processing personal data on a controller's behalf — host, email platform, payroll bureau.
- **Profiling** — Automated evaluation of personal aspects — behaviour, preferences, performance, location.
- **Pseudonymisation** — Replacing identifiers so data can't be attributed without a separately kept key. A safeguard, not an exemption.
- **Restriction of processing** — Freezing data — stored but untouched — while a dispute or verification is pending (Article 18).
- **SCCs** — Standard Contractual Clauses — the Commission's template contracts that make third-country transfers lawful.
- **Special categories** — Health, biometric, genetic, religious, political, sexual-life and trade-union data (Article 9).
- **Supervisory authority** — Your national data protection regulator — AZOP, CNIL, the Irish DPC, and peers.
- **Transfer Impact Assessment** — The documented check that a destination country's laws don't undermine your SCCs in practice.
- **72-hour rule** — The Article 33 deadline for notifying your authority of a reportable breach, counted from awareness.

APPENDIX B

Your first 30 days, week by week

The 20-point checklist tells you *what*; this plan tells you *when*. It assumes roughly two focused hours per working day from one owner, with short check-ins from management.

Week 1 — See clearly (points 1–3)

Inventory every system holding personal data: walk through a customer's lifecycle from first contact to invoice and note every tool it touches — CRM, inbox, forms, analytics, payroll, backups, spreadsheets. Draft your Article 30 record directly from that walk-through, one row per activity. Name the privacy owner and put a recurring monthly slot in their calendar.

Week 2 — Justify (points 4–7)

For each RoPA row, record the lawful basis. Write the balancing test for every legitimate-interest row — three honest paragraphs each. Flag any special-category data and either document its Article 9 condition or stop collecting it. Mark every non-EU vendor and check its transfer mechanism: DPF certification, SCCs, or adequacy.

Week 3 — Publish and contract (points 8–11)

Rewrite or generate your privacy notice from the RoPA — they must match. Fix the cookie banner so 'reject' equals one click. Collect signed DPAs from every processor into one folder; chase the missing ones. Set a retention period on every RoPA row and delete what's already past it.

Week 4 — Prepare for bad days (points 12–20)

Stand up the breach register and response plan (Chapter 14), create the data subject request templates and intake address, run a one-hour breach tabletop and a test access request, switch on MFA everywhere, and hold a 30-minute all-hands on the new rules — including what may and may not be pasted into AI tools. Close by filing all evidence in one accountability folder and booking the annual review.

Day 30 outcome: a defensible baseline — documented processing, justified bases, published notices, contracted processors and a rehearsed incident plan. From here, compliance is maintenance, not a mountain.

APPENDIX C

Supervisory authorities: who regulates you

Your lead authority is in the member state of your main establishment. For breach notifications, complaints and DPIA consultations, these are the front doors — every authority publishes notification forms and SMB guidance.

- **Croatia** — AZOP · azop.hr
- **Germany** — federal BfDI plus one authority per Land; find yours via bfdi.bund.de (companies answer to the Land authority of their seat)
- **France** — CNIL · cnil.fr (exceptional SMB toolkits and model records)
- **Ireland** — Data Protection Commission · dataprotection.ie
- **Netherlands** — Autoriteit Persoonsgegevens · autoriteitpersoonsgegevens.nl
- **Spain** — AEPD · aepd.es (free Facilita tool for low-risk SMBs)
- **Italy** — Garante · garanteprivacy.it
- **Austria** — DSB · dsb.gv.at
- **Belgium** — APD/GBA · autoriteprotectiondonnees.be
- **Poland** — UODO · uodo.gov.pl
- **Portugal** — CNPD · cnpd.pt
- **Sweden** — IMY · imy.se
- **EU level** — European Data Protection Board · edpb.europa.eu (guidelines cited throughout this guide)

Bookmark your authority's breach notification form today — you do not want to be searching for it at hour 70 of 72.

APPENDIX D

The ten questions a regulator asks first

When an authority contacts a business — after a complaint, a breach, or a sweep — the opening questionnaire is remarkably consistent. If you can answer these ten questions with documents rather than improvisation, the interaction usually ends quickly.

- **1. 'Provide your record of processing activities.'** — The Article 30 RoPA, current and complete. This is almost always request number one.
- **2. 'What is your lawful basis for this processing?'** — Named per activity, with the balancing test attached where it's legitimate interest.
- **3. 'Show us the information you gave data subjects.'** — Your privacy notice, and proof of when and where it was presented.
- **4. 'How was consent obtained?'** — Screenshots of the actual form and banner, plus stored consent records with timestamps.
- **5. 'List your processors and provide the agreements.'** — The vendor register and signed DPAs.
- **6. 'Is personal data transferred outside the EEA, and on what basis?'** — The transfer map: destination, mechanism, TIA where SCCs are used.
- **7. 'What are your retention periods and how are they enforced?'** — The schedule, and evidence deletion actually happens.
- **8. 'Describe your technical and organisational security measures.'** — Access control, encryption, MFA, backups, training — at the level of a two-page summary.
- **9. 'Provide your breach register.'** — Including incidents you assessed as non-reportable, with the reasoning.
- **10. 'How do you handle data subject requests?'** — The intake channel, the log, and response times against the one-month clock.

Reading back through this list, notice what it is: the 20-point checklist in interrogative form. A regulator's first letter is an open-book exam — and this guide is the book.

YOU MADE IT

From regulation to reality

GDPR compliance is not a project you finish; it is an operating habit with an annual rhythm. But the gap between 'we should look into that someday' and 'we are demonstrably compliant' is smaller than it looks — for most SMBs it is the 20 points in Chapter 13, done honestly, over a few working days.

Keep going with the free tools

- **GDPR Compliance Checker** — your instant score and prioritised action plan · gdprgard.eu/gdpr-audit
- **Privacy Policy Generator** — Articles 13–14 covered, in your language · gdprgard.eu/privacy-generator
- **BreachNotify** — 72-hour assessment and notifications · gdprgard.eu/breachnotify
- **VATGuard, ContractGuard, HRForge and more** — the full suite · gdprgard.eu