GDPRGARD.EU · FREE GUIDE

Controller vs *Processor.*

The complete GDPR guide to Article 4(7), 4(8) and 26 — the purposes-and-means test, joint controllers, ten worked examples, Article 28 processor obligations, sub-processor liability, and a decision flowchart you can run today.

GDPRGard.eu

2026 Edition

Table of Contents

1. Why This Is the First Question, Not a Footnote

Before a business can write a privacy policy, sign a data processing agreement, or answer a subject access request, it has to answer a more basic question: under the GDPR, are we a **controller** or a **processor** for this particular set of personal data?

Most businesses skip this question, or answer it once and never revisit it. That is a mistake, because almost every other GDPR obligation flows downstream from this one classification. Controllers decide *why* and *how* data is processed, and carry the primary legal duty to justify that processing, inform data subjects, and respond to their rights. Processors act *only* on a controller's documented instructions, and carry a narrower — but still real, and since 2018 directly enforceable — set of duties around security, sub-processing, and assistance.

Get the label wrong, and everything built on top of it is wrong too: the wrong party signs the wrong contract, the wrong party keeps the wrong records, and when a regulator or a data subject comes asking, the business that assumed it was "just a processor" discovers it was legally a controller the entire time — with direct liability for lawful basis, transparency, and every other controller-only obligation it never met.

> **Who this guide is for:** any business that handles personal data on behalf of, alongside, or in service of another business — SaaS vendors, marketing agencies, payroll and HR platforms, IT support providers, freelancers with client data, and any company evaluating a new vendor relationship. If you have never explicitly decided which role you play for each processing activity, this guide is for you.

This is not an academic distinction invented by lawyers to sell more contracts. The European Data Protection Board (EDPB) has issued dedicated guidance on it (Guidelines 07/2020), national regulators have fined businesses specifically for misclassifying themselves, and courts have overturned "we thought we were just a processor" defences when the facts showed otherwise. The rest of this guide works through the legal test, the practical worked examples, the contracts you need, and a checklist you can run today.

2. Controller Defined: Article 4(7) and the "Purposes and Means" Test

Article 4(7) GDPR defines a controller as the natural or legal person, public authority, agency, or other body which, **alone or jointly with others, determines the purposes and means of the processing of personal data**.

Two words carry the entire legal weight of this definition: **purposes** and **means**.

Purposes means the *why* — the business reason the data is being processed at all. A retailer collects customer email addresses to fulfil orders and to send marketing emails. A hospital processes patient records to provide care and to bill insurers. The purpose is the outcome the organisation is actually trying to achieve.

Means means the *how* — the essential decisions about the way processing happens. The EDPB distinguishes between "essential means" (which categories of data are collected, how long they're kept, who can access them, which third parties receive them — decisions that are so closely tied to the purpose that they are effectively part of it) and "non-essential means" (the specific software used, the server configuration, the exact security measures — operational choices that can be delegated without changing who is legally in control).

A party is a controller if it determines the purposes of processing — full stop, regardless of who determines the means. A party is *also* a controller (not merely a processor) if it determines the essential means, even where another party decided the purpose. This is why "we don't decide why the data is collected, we just decide how it's stored and secured" is not automatically a processor defence — if the "how" decisions being made are essential ones, that party is a controller for those decisions.

Controllers do not need a contract with data subjects, and they do not need to be first in the chain. A recruitment agency that decides which candidate data to collect, how long to retain it, and which employers to share it with is a controller — even though the individuals never signed anything with the agency directly, and even though the agency is itself acting for client employers.

What makes someone a controller — indicators from EDPB guidance

- Legal provision expressly designates the organisation as responsible (e.g., an employer for employee payroll data, a bank for AML checks)
- The organisation decided to collect the data in the first place
- The organisation decided which categories of data subjects and data to collect
- The organisation decided the purpose for which the data would be used
- The organisation decided which third parties can access the data
- The organisation decided the retention period
- The organisation benefits from the processing in a way that goes beyond simply being paid a service fee

No single factor is decisive. The test is a factual, substance-over-form assessment of *who actually calls the shots* — not what the contract between the parties happens to say. A written agreement labelling a company "the processor" does not make it one if, in practice, that company decides why and how the data is used.

3. Processor Defined: Article 4(8) and the Line You Cannot Cross

Article 4(8) GDPR defines a processor as a natural or legal person, public authority, agency, or other body which **processes personal data on behalf of the controller**.

The defining feature of a processor is that it has **no purpose of its own** for the data. It processes personal data strictly to deliver a service to the controller, following the controller's documented instructions, and does not decide why the data is collected or what happens to it beyond what it was told to do.

Classic processor relationships include:

- A cloud hosting or infrastructure provider storing a client's customer database
- A payroll bureau processing salary data exactly as instructed by the employer
- An email marketing platform sending campaigns designed and targeted by the controller
- A call-centre operator handling customer service calls on a company's behalf
- An IT support contractor with access to a client's systems for maintenance purposes only

The line a processor cannot cross: the moment a processor starts making its own decisions about *why* or in ways that go beyond the controller's instructions — using customer data collected for one client to improve its own product for other clients, retaining data longer than instructed because it finds it useful, or repurposing data for its own analytics or advertising — it stops being a processor for that activity and becomes a controller (often without realising it, and often in violation of both GDPR and its own customer contract).

This is the single most common way vendors accidentally become controllers: a SaaS company hosts customer data purely to deliver the service (processor), but also uses aggregated or even identifiable data from that same dataset to train its own models, benchmark its own product, or build cross-customer analytics products (controller, for that specific use). Many companies are legitimately a **processor for one purpose and a controller for another**, with respect to the *exact same underlying dataset* — the classification is per-processing-activity, not per-company.

> **Practical test:** ask "if the controller instructed us to stop this specific use of the data tomorrow, could we comply without affecting anything else we do with it?" If yes, that use is being carried out as a processor. If the answer is "no, because we rely on it for our own purposes," that use makes you a controller for it.

Processors are not off the hook simply because they are not "in charge." Since the 2018 GDPR came into force, processors carry **direct, independently enforceable obligations** under Article 28 (discussed in Chapter 7) and can be fined by regulators in their own right — not only through the controller.

4. Joint Controllers: When Two Businesses Share the Decision (Article 26)

Article 26 GDPR covers situations where **two or more controllers jointly determine the purposes and means of processing**. This is distinct from a controller-processor relationship: joint controllers are not one giving instructions to the other — both parties are genuinely deciding *together*, even if their involvement or level of control is unequal.

Common joint-controller scenarios:

- **Platform and merchant**, where a marketplace and a seller both determine how buyer data is used (the platform for account and payment purposes, the seller for order fulfilment) and both benefit
- **Co-organisers of an event**, where two companies jointly decide who to invite and what data to collect on attendees
- **Franchisor and franchisee**, where the franchisor sets group-wide data policies that the franchisee implements with some independent decision-making of its own
- **Employers using shared recruitment or benefits platforms**, where both the platform and employer make substantive decisions about candidate or employee data

The CJEU's *Wirtschaftsakademie* and *Fashion ID* rulings (both concerning Facebook plugins and fan pages) established that joint controllership can exist even when one party has **no access to the underlying data at all** — it is enough that the party helped determine the purpose and means of a stage of the processing, such as embedding a tracking pixel that collects visitor data for both parties' benefit.

Joint controllers must set out their respective responsibilities in a transparent arrangement — who handles subject access requests, who provides the privacy notice, who is the primary contact for data subjects — and Article 26(3) makes clear that data subjects can exercise their rights against **either** joint controller, regardless of what the internal arrangement says. The arrangement governs the parties' internal relationship, not what a data subject is entitled to expect.

Joint controllership is easy to fall into by accident — shared marketing platforms, co-branded lead generation forms, and integrated partner tools are common sources — and it is worth deliberately checking for it whenever two organisations both touch the same dataset for related but not identical purposes.

5. The Test in Practice: Ten Worked Examples

Legal definitions become useful once applied to situations that look like the ones your business is actually in. Ten common scenarios, worked through:

1. E-commerce store and its payment processor (Stripe, Adyen, etc.) The store is the controller of checkout data. The payment processor is generally a controller in its own right for fraud prevention, regulatory compliance, and its own service purposes — payment processors are a well-established exception to the "processor" label because payment services law imposes independent obligations on them.

2. SaaS company and its cloud infrastructure provider (AWS, Azure, GCP) The SaaS company is the controller. The cloud provider is a processor (or sub-processor, if the SaaS company itself is a processor for its own customers) — it stores and processes data purely to deliver infrastructure, with no purpose of its own for the content.

3. Marketing agency running campaigns for a client If the agency executes campaigns strictly per the client's brief using the client's contact lists, it is a processor. If the agency also builds its own prospect databases, decides which audiences to target using its own judgment and proprietary data, or reuses client data to improve its own tools, it is a controller for those activities — commonly making agencies **joint controllers with their clients** for campaign data.

4. Payroll bureau processing employee salaries Processor. The bureau calculates and pays salaries exactly as instructed by the employer, which remains the controller and decides what data is collected, retained, and shared with tax authorities.

5. Accountant preparing a client's annual accounts Controller, not processor — despite the "service provider" framing that many accountants assume applies. Professional accountants exercise independent professional judgment about which data to collect and how to treat it under their own professional obligations; they are not simply following the client's instructions.

6. Law firm advising a client Controller, for the same reason as accountants: legal professionals exercise independent judgment and owe independent professional duties that go beyond following client instructions.

7. IT support contractor with remote access to fix technical issues Processor, provided access is limited to what is necessary for support and the contractor does not repurpose anything it sees. This is one of the most common processor relationships and one of the most commonly undocumented with a proper DPA.

8. Recruitment agency sourcing candidates for an employer Typically a controller for the candidate pool it builds and maintains (it decides which candidates to add, how long to keep them, who else to present them to) and acts more like a processor only for the specific placement process on behalf of one client — in practice, most recruitment agencies are controllers.

9. Email marketing platform (Mailchimp-style tool) Processor for the emails and lists a customer builds and sends through it. Becomes a controller if it uses customer data for its own deliverability scoring, spam analytics, or product development beyond what is necessary to deliver the sending service.

10. Two hospitals sharing a patient referral system Likely joint controllers — both determine why and how referral data is processed, both have independent obligations to the patient, and neither is simply following the other's instructions.

The consistent thread: **"we were paid to do it" does not settle the question.** What settles it is who decided the categories of data, the purpose, the retention, and the downstream sharing.

---

6. Why the Label Matters: Liability, Fines, and Who Regulators Call First

Getting the classification right is not a compliance-paperwork exercise — it determines who is legally exposed, and how much.

Controllers carry the primary legal burden. They must establish a lawful basis for every processing purpose (Article 6), provide privacy notices (Articles 13–14), honour data subject rights (Articles 15–22), conduct DPIAs where required (Article 35), and are the default first point of contact for both regulators and data subjects. When something goes wrong — an unlawful marketing email, a botched subject access request, a breach caused by inadequate organisational measures — the controller is answerable even if a processor's system was where the failure technically occurred.

Processors carry direct, independently enforceable duties since 2018. Article 28(3) processor obligations, Article 32 security requirements, and breach-notification duties to the controller are not merely contractual — supervisory authorities can investigate and fine processors directly for failing them, without needing to go through the controller first. A processor that ignores its DPA, appoints unauthorised sub-processors, or fails to notify a breach promptly is exposed in its own right.

Both roles are subject to the same maximum fine tiers under Article 83 — up to €20 million or 4% of global annual turnover for the most serious infringements, whichever is higher, and up to €10 million or 2% for the lower tier (which specifically includes Article 28 processor-obligation breaches). The idea that "processors face lighter penalties" is a myth; what differs is *which obligations* each role is fined for, not the ceiling.

Joint controllers face the sharpest exposure of all. Article 26(3) allows a data subject to bring a claim against either joint controller for the *full* amount of any damage, regardless of the internal split of responsibility agreed between the parties — the injured party does not have to sort out which controller was more at fault. The joint controllers then settle the apportionment between themselves afterward.

Practical consequence for contract negotiation: vendors frequently push to be labelled "processor" in contracts because it appears to limit their exposure, and customers frequently accept this without checking whether it matches reality. If a regulator or a court later determines that the vendor was, in substance, a controller — because it made essential decisions about the data — the contractual label provides no protection. Classify based on the facts, not on which label is commercially convenient for either party.

7. Processor Obligations Under Article 28

Article 28 GDPR sets out the mandatory content of any processing arrangement and the direct obligations a processor carries. A processor must:

1. **Only process personal data on the controller's documented instructions** — including with regard to transfers to third countries — unless required to do otherwise by EU or member state law, in which case it must inform the controller before processing (unless that law prohibits such notice on important public interest grounds)
2. **Ensure persons authorised to process the data are bound by confidentiality**, whether by statute or contractual obligation
3. **Implement appropriate technical and organisational security measures** under Article 32, on the same risk-based standard that applies to controllers
4. **Respect the conditions for engaging a sub-processor** (see Chapter 9) — general or specific written authorisation, and flow-down of equivalent data protection obligations
5. **Assist the controller in responding to data subject rights requests**, taking into account the nature of the processing, by appropriate technical and organisational measures insofar as this is possible
6. **Assist the controller with its Article 32–36 obligations** — security, breach notification, DPIAs, and prior consultation with the supervisory authority — taking into account the nature of processing and the information available to the processor
7. **Delete or return all personal data at the end of the service**, at the controller's choice, and delete existing copies unless EU or member state law requires storage
8. **Make available to the controller all information necessary to demonstrate compliance**, and allow for and contribute to audits, including inspections, conducted by the controller or an auditor it mandates

Article 28(10) contains a provision that catches many vendors by surprise: **if a processor determines the purposes and means of processing in breach of its instructions, it is treated as a controller for that processing** — meaning it loses whatever protection the processor role offered and takes on full controller liability retroactively for that activity.

A processor's obligations exist independently of whether they were remembered to be written into the contract. Article 28(3) requires that processing by a processor be governed by a contract or other legal act — but the *substantive* duties in the list above apply regardless, because they are statutory, not merely contractual.

8. What a Compliant Data Processing Agreement Must Actually Contain

A Data Processing Agreement (DPA) is the legal instrument required by Article 28(3) whenever a controller uses a processor. Many businesses have *a* document called a DPA in their files without checking whether it actually satisfies the statutory minimum content — a generic NDA-style confidentiality clause, or a one-paragraph mention of "GDPR compliance" in a master services agreement, does not meet the bar.

Mandatory content under Article 28(3)

- **The subject matter and duration of the processing** — what this specific engagement covers and for how long
- **The nature and purpose of the processing** — described specifically enough to be meaningful, not "as necessary to provide the services"
- **The type of personal data and categories of data subjects** — e.g. "names, email addresses, and order history of the controller's customers," not just "personal data"
- **The controller's obligations and rights**
- A binding instruction that the processor **processes data only on the controller's documented instructions**, including for international transfers
- Confirmation that persons processing the data are **under a duty of confidentiality**
- Confirmation of the **security measures** implemented under Article 32
- The **conditions for engaging sub-processors** (see Chapter 9)
- **Assistance obligations** for data subject rights, breach notification, DPIAs, and prior consultation
- The **end-of-contract data return or deletion** obligation
- **Audit and inspection rights** for the controller, and the processor's obligation to make compliance information available

Practical red flags when reviewing a vendor's proposed DPA

- Processing purposes described so broadly they could cover anything ("as needed for the services") — this fails the specificity requirement and gives the processor de facto discretion, which points toward controller status regardless of the label
- No named sub-processors or sub-processor list, and no mechanism to be notified of new ones
- Security measures section that just says "industry standard" with no Article 32-specific detail
- No audit rights, or audit rights limited to a vendor-controlled questionnaire with no ability to escalate
- International transfer terms that reference outdated mechanisms (Privacy Shield, pre-2021 SCCs) instead of the current EU Standard Contractual Clauses or an adequacy decision
- A "processor" DPA for a relationship that, per Chapter 5's test, is actually controller-to-controller or joint controllership — signing the wrong type of agreement does not change the underlying legal facts, but it does mean neither party has documented the arrangement correctly

The EU Commission's **Standard Contractual Clauses for controller-processor relationships** (distinct from the SCCs used for international transfers) provide a pre-approved template that satisfies Article

28(3) and can be used or adapted directly, which is the safest starting point for most SMBs rather than drafting from scratch.

---

9. Sub-Processors: Authorisation, Notification, and the Liability Chain

Most processors do not do everything in-house — a SaaS company uses a cloud host, an email platform uses a delivery infrastructure provider, an agency uses a specialist analytics tool. Each of these downstream vendors that also processes the controller's personal data is a **sub-processor**, and Article 28(2) and 28(4) govern how they must be handled.

Authorisation. A processor may only engage a sub-processor with the controller's **prior authorisation**, which can be either:

- **Specific authorisation** — the controller approves each named sub-processor individually, or
- **General written authorisation** — the controller pre-approves the processor's use of sub-processors generally, on condition that the processor **informs the controller of any intended changes** (adding or replacing a sub-processor) with enough advance notice that the controller has a genuine opportunity to object

Most SaaS vendors use general authorisation with a published sub-processor list and a notification mechanism (email alerts or a status page) — this is compliant provided the notice period is real and objections are genuinely considered, not a formality.

Flow-down obligations. Article 28(4) requires that the same data protection obligations set out in the controller-processor DPA be imposed on the sub-processor by contract — in particular, sufficient guarantees to implement appropriate technical and organisational measures. The processor cannot simply hand data to a sub-processor under weaker terms than it agreed to with the controller.

Liability. This is the point most businesses get backwards. **The processor remains fully liable to the controller for the sub-processor's performance**, as if the processor had performed those obligations itself (Article 28(4), last sentence). A controller does not need to chase a sub-processor it never contracted with directly — it holds its processor accountable, and the processor in turn holds the sub-processor accountable under their own contract.

Practical due diligence for a business acting as controller:

1. Ask every processor for its current sub-processor list before signing
2. Confirm the notification mechanism for new sub-processors and how much time you have to object
3. Check that sub-processors handling data outside the EU/EEA have a valid transfer mechanism (see Chapter 10)
4. Understand that objecting to a new sub-processor may be a contractual right to terminate rather than a veto — read the specific clause

10. International Transfers: Controller Duties vs Processor Duties

When personal data moves outside the EEA to a country without an adequacy decision, both controllers and processors have obligations — but they are not identical.

The controller decides whether a transfer happens at all. It is the controller's responsibility to identify that a transfer is occurring (including indirect transfers, such as remote access from a third country to data stored in the EU, which counts as a transfer under current EDPB guidance) and to put a valid transfer mechanism in place — Standard Contractual Clauses, an adequacy decision, Binding Corporate Rules, or a narrow Article 49 derogation.

The processor must not transfer data outside the controller's instructions. Article 28(3)(a) explicitly extends the "documented instructions only" rule to international transfers — a processor cannot decide on its own to move data to a sub-processor or data centre outside the EEA without that being covered by the controller's instructions and a valid transfer mechanism being in place.

Where it gets complicated: processor-to-sub-processor transfers. If a controller in the EU uses a processor in the EU, but that processor uses a sub-processor outside the EEA, a transfer has occurred and needs its own legal basis — typically SCCs between the processor and sub-processor, with the controller's authorisation. This is a common gap: businesses check their direct vendor's location but not their vendor's vendors.

Transfer Impact Assessments (TIAs). Since the *Schrems II* ruling, using SCCs is not automatically sufficient — the party relying on them must assess whether the destination country's laws (particularly government surveillance powers) undermine the protections the SCCs promise, and add supplementary measures (such as strong encryption with keys held outside the destination country) if needed. This obligation falls primarily on the controller as the party responsible for the transfer, but a processor initiating a sub-processor transfer on the controller's behalf should support this assessment as part of its Article 28(3)(f) assistance duty.

11. The Misclassifications That Get Businesses in Trouble

Patterns that recur across enforcement decisions and real-world vendor disputes:

"We're just a processor" as a blanket excuse. A vendor assumes processor status protects it from having to think about lawful basis, transparency, or data subject rights at all — then discovers that for one specific use of the data (its own analytics, its own marketing to end users, its own AI training), it was acting as a controller the whole time, with none of the controller obligations met for that activity.

No DPA at all, because "it's covered in the main contract." A general services agreement with a paragraph mentioning "the parties will comply with applicable data protection law" does not satisfy Article 28(3)'s specific mandatory content requirements. This is one of the most common findings in regulatory investigations and is often the first thing a DPA asks to see.

Treating internal group companies as automatically exempt. There is no "corporate family" exception in the GDPR — a parent company processing a subsidiary's customer data, or vice versa, needs the same controller/processor/joint-controller analysis and the same documentation as any external relationship, including intra-group data transfer agreements.

Assuming a free tool has no controller obligations because "nothing is being sold." Whether money changes hands is irrelevant to controller status — a free browser extension, a free CRM tier, or an internal HR tool built by an IT team all trigger controller obligations if personal data is processed, regardless of price.

Confusing "we don't look at the data" with "we're a processor." Automated or encrypted processing without human viewing of content does not by itself determine the role — a zero-access encrypted backup provider is typically still a processor because it does not decide purposes or essential means, but the "we never look at it" fact alone is not what makes that true.

Not revisiting the classification when the product changes. A tool that started as pure infrastructure (processor) often accumulates controller-style features over time — usage analytics, AI features trained on customer content, cross-customer benchmarking — without anyone updating the DPA or the underlying legal analysis to match.

12. Decision Flowchart: Am I a Controller, a Processor, or Both?

Work through these questions **for each specific processing activity** — not once for your whole business, since the same company is routinely a processor for one activity and a controller for another.

Step 1 — Who decided why this data is being processed at all? If your organisation decided the business purpose (not merely executed someone else's decision), you are at minimum a controller for this activity. Go to Step 4. If another organisation decided the purpose and you are only delivering it, continue to Step 2.

Step 2 — Do you decide any "essential means"? Essential means include: which categories of data are collected, how long data is retained, who else can access it, or which third parties receive it. If you make any of these decisions independently rather than following documented instructions, you are a controller (or joint controller) for this activity. Go to Step 4. If all of these were decided by the other party and you simply follow instructions, continue to Step 3.

Step 3 — Do you ever use this data for a purpose of your own (product improvement, your own analytics, your own marketing, AI training) **beyond delivering the instructed service?** If yes, you are a controller for that specific additional use, even while remaining a processor for the primary service. Document both roles separately. If no, you are a processor for this activity. Confirm a compliant DPA is in place (Chapter 8) and stop here.

Step 4 — Is another organisation also making purpose-or-essential-means decisions about the same data, at the same time, for related aims? If yes, you are likely joint controllers under Article 26 — set out a transparent arrangement covering who handles data subject requests and who provides the privacy notice (Chapter 4). If no, you are a sole controller — establish lawful basis, provide a privacy notice, and prepare to handle data subject rights directly.

Run this per relationship, per dataset, and revisit it whenever a product or contract changes materially.

13. 15-Point Checklist: Documenting Your Role Correctly

Use this to audit your organisation's classification for each significant data relationship — not as a one-time exercise, but as a template to repeat whenever a new vendor, product feature, or partnership is added.

Classification

1. ☐ Every significant processing activity has an explicit controller/processor/joint-controller classification on record, not assumed
2. ☐ The classification was based on who actually decides purposes and essential means — not on which label was commercially convenient
3. ☐ Classifications are reviewed when a product, vendor relationship, or data use changes materially

If you are a controller 4. ☐ A lawful basis is documented for every purpose of processing 5. ☐ A privacy notice covers the processing and is actually provided to data subjects 6. ☐ A process exists for handling data subject rights requests within the one-month statutory deadline 7. ☐ Every processor you use has a compliant Article 28(3) DPA on file

If you are a processor 8. ☐ You process data only per the controller's documented instructions, with no undocumented secondary uses 9. ☐ Staff with data access are bound by confidentiality obligations 10. ☐ Article 32 security measures are implemented and can be evidenced on request 11. ☐ A current sub-processor list exists and controllers are notified of changes with a real objection window 12. ☐ A process exists to assist controllers with data subject requests, breaches, and DPIAs within a reasonable timeframe 13. ☐ End-of-contract data deletion or return is a defined, tested process, not an afterthought

If you are (or might be) a joint controller 14. ☐ A transparent Article 26 arrangement exists, naming who provides the privacy notice and who is the primary contact for data subjects 15. ☐ Both parties understand that a data subject can claim against either of them for the full amount of any damage, regardless of the internal split

14. About GDPRGard

This guide is provided free by **GDPRGard.eu** — a platform that helps small and mid-sized businesses meet their GDPR obligations without hiring a full-time compliance team. Our self-serve tools generate GDPR-compliant contracts — including Article 28 Data Processing Agreements — breach notification letters, privacy policies, and DPIAs in minutes, and our free resources — checklists, calculators, and guides like this one — are built to be genuinely useful on their own, whether or not you ever become a customer.

Explore the rest of our free tools at gdprgard.eu.

This guide is provided for general informational purposes only and does not constitute legal advice. Whether a specific organisation is a controller, processor, or joint controller depends on the facts of its actual processing activities; consult a qualified data protection professional or lawyer for advice tailored to your organisation.