TrustArc

PRIVACY POWERUP

Welcome to the Privacy PowerUp Series — your go-to toolkit for mastering the privacy fundamentals. Level up your knowledge and explore every resource in the series.

Decoding Data Processing Agreements (DPAs)

The 10 Most Negotiated Provisions in a DPA

Think a DPA is just a legal formality? Think again.

Behind every clause is a negotiation about risk, compliance, and accountability. Here's a visual walkthrough of the most hotly debated Data Processing Agreement provisions and why they matter.

1. Scoping Considerations

What data is being processed, how, and by whom?

- Is it customer PII, HR data, or health records? Different categories demand different controls.
- Is data just being stored or enriched, profiled, or analyzed?
- The controller–processor relationship defines responsibility.
- Scoping is the foundation of the DPA and often revisited multiple times.

Tip: Nail this down early. Vague scoping = downstream negotiation drama.

2. Limitations on Use

How narrowly (or broadly) should the processor use the data?

- Controllers want strict limits to avoid misuse.
- Processors want flexibility for analytics, ML training, or operational improvements.
- Too narrow? You stifle innovation.
- Too broad? You risk violations and misalignment with GDPR.

Tip: Strike a balance with clear language on purpose, retention, and deletion.

3. Subprocessor Authorization

Who's allowed in the data supply chain?

- Article 28(2) requires controller approval for subprocessors.
- Choose between:
  - *Specific Authorization:* Case-by-case approval
  - *General Authorization:* Pre-approval with opt-out rights
- Define how objections are handled and whether they trigger termination rights.

Tip: Modern vendor ecosystems are complex. Controllers want visibility, and processors want agility.

4. Security Incident Notification

How fast is "without undue delay"?

- Controllers often push for specific timelines (e.g., "within 24 hours").
- Processors may hesitate due to dependencies on third parties.
- Define what qualifies as a notifiable incident — only confirmed breaches, or also attempted intrusions?

Tip: In a crisis, vagueness = chaos. Build in precision and paths to escalation.

5. Security Incident Remediation

After the breach… then what?

- Who takes the lead? Who approves remediation measures?
- Are controllers involved in the response plan?
- Who's the point of contact on each side?

Tip: Your DPA should guarantee transparency, not bottlenecks.

6. Audit Rights

How can controllers verify compliance?

- Controllers want the right to audit.
- Processors prefer offering **SOC 2 Type 2** or **ISO 27001** reports in lieu of on-site visits.
- Negotiations often focus on:
  - Timing and frequency
  - Who pays
  - Scope and confidentiality protections

Tip: Trust but verify, and agree on terms that won't crush operations.

7. Indemnity & Limitation of Liability

Who pays when things go wrong?

- Controllers want indemnity for:
  - Security incidents
  - Non-compliance
  - Third-party claims
- Processors push to **limit liability** often to the value of the contract or 2x its amount.

Tip: This is usually the final and fiercest negotiation. Get legal involved early.

8. Standard Contractual Clauses (SCCs)

Cross-border data transfers need more than a checkbox.

- SCCs are a must-have unless there's an adequacy decision.
- Debate centers on:
  - Which optional clauses to include
  - How detailed the Annexes I–III should be (especially TOMs and data flows)

Tip: Post-Schrems II, "fill in later" is not a strategy. Precision matters.

9. Data Subject Access Requests (DSARs)

Support vs. overload: where's the line?

- Processors must assist controllers per GDPR Article 28(3)(e).
- But what does "assist" mean?
  - Identity verification?
  - Redactions?
  - Secure handoffs?

Tip: Controllers want speed. Processors fear back-office overload. Spell it out.

10. Technical & Organizational Measures

The security backbone of the DPA.

- Whose TOMs apply: the controller's, the processor's, or both?
- Controllers want detail. Processors want flexibility (especially at scale).
- Be clear about:
  - Encryption, access controls, monitoring, and incident response
  - Customization for high-risk activities

Tip: Controllers want speed. Processors fear back-office overload. Spell it out.

A DPA isn't just paperwork. ***It's a living agreement where data risk is allocated, regulated obligations are operationalized, and trust is built or broken.***

Want more privacy power moves? Explore the full Privacy PowerUp Series for infographics, articles, and videos that put you in control.