



Vendor Management Essentials

Know Your Role, Control the Risk



You can outsource processing, but not accountability

Controllers may delegate data processing to vendors (processors), who may even subcontract (sub-processors) — but controllers stay accountable for:

- ✓ Choosing the right vendor
- ✓ Ensuring compliance
- ✓ Monitoring over time

A handshake isn't enough. Get your DPA in writing.

A binding **Data Processing Agreement (DPA)** is required. Be sure it includes:



Purpose of processing



Type of data involved



Processing instructions



Duration of service



Mutual obligations

Before you sign, scrutinize your processor.

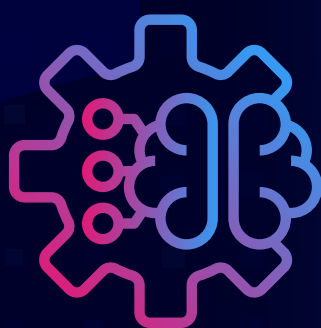
Vet vendors using this privacy-first due diligence list:

1. Expertise & capacity
2. Jurisdiction & access risks
3. Reputation in the market
4. Data breach history
5. Regulatory record
6. Employee turnover
7. Customer satisfaction
8. Privacy program in place

Is your vendor's AI processing your data?

Ask your vendors:

- Does their AI use your data to train models?
- Are humans in the loop?
- Is the AI legally compliant and bias-monitored?
- Are they transparent with you and data



Don't just onboard. Stay on guard.

Your oversight never ends:

- Regularly assess vendor risk
- Send tailored questionnaires
- Conduct risk-based audits
- Track changes in processing
- Build a reusable audit question library



SELECT



CONTRACT



MONITOR



AUDIT

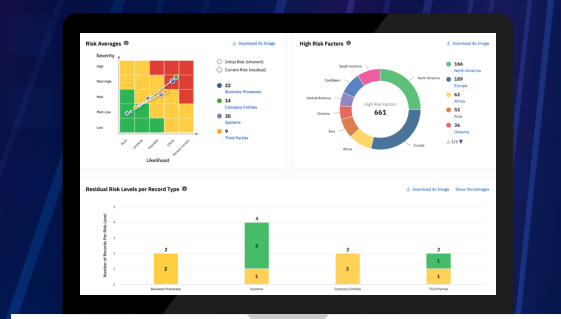


ADJUST

PowerUp Your Vendor Management



Data Mapping & Risk Manager



- ✓ Automate data flow mapping
- ✓ Capture vendor risk
- ✓ Score and track compliance
- ✓ Generate reports on demand

Get control and prove it.

REQUEST A DEMO

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