

CONTRACTS

Data Processing Agreements

The UK GDPR terms required when a supplier handles personal data on your behalf, and how to check what you've already signed.

Controllers and processors

Under the UK GDPR, a controller decides why and how personal data is used. A processor handles it on the controller's behalf and on its instructions. Typical processors for a small business are the payroll bureau, the cloud accounting provider, the IT support company, the mailing platform and the outsourced HR service.

When a processor handles personal data for a controller, the law requires a written contract between them (Article 28 of the UK GDPR). This is usually called a data processing agreement, or DPA. The requirement applies to the controller. Without the contract, the controller is in breach, even if the processor does nothing wrong.

What the agreement must say

In outline, the contract must set out:

- the subject matter and duration of the processing
- its nature and purpose
- the type of personal data and the categories of data subject
- that the processor acts only on the controller's documented instructions
- that people who handle the data are bound by confidentiality
- the security measures the processor will take
- when the processor may use a sub-processor, and that the controller must authorise it
- how the processor will help the controller respond to individuals' rights requests
- how the processor will help with security, breach notification and impact assessments
- that the data is deleted or returned at the end of the services
- that the processor will make available information and allow audits

Most suppliers publish a standard DPA. It is still the controller's responsibility to check it is adequate.

What the regulator expects

The Information Commissioner's Office expects organisations to know where their data goes and who handles it. A supplier list, a record of processing activities and signed contracts are the basic evidence.

Key points

- A written contract is a legal requirement when a processor handles personal data.
- The controller carries the risk if it is missing.
- Check sub-processors and where data is held.
- Transfers outside the UK need a lawful mechanism.
- Know which suppliers have personal data.
- Review the contracts when services change.

Checking what you have already signed

A short review will show where the gaps are.

1. **List the suppliers** that handle personal data on your behalf: payroll, accounting software, cloud storage, email, marketing, CRM, HR and IT.
2. **Find each contract or online terms.** Many DPAs are part of the supplier's standard terms, accepted when you signed up.
3. **Check each against the list above.** Missing instructions, security, sub-processor or deletion terms are the usual gaps.
4. **Check international transfers.** If the data goes outside the UK, check which mechanism is used, such as an adequacy decision or standard contractual clauses.
5. **Record it.** Keep a register of suppliers, what data they hold, and where the DPA is.
6. **Chase the gaps.** Ask the supplier for its DPA or negotiate changes if the data is sensitive.

Before you start

- Who handles personal data for us?
- Do we have a DPA with each?
- Does it cover sub-processors and deletion?
- Does data leave the UK?
- Who keeps the register?
- When was the privacy notice reviewed?

Controller or processor?

The label in the contract does not decide the role. A supplier that decides for itself how data is used may be a controller, or a joint controller. Where roles are unclear, record the analysis.

Recent changes

Data protection law has been updated by recent legislation, and regulators' guidance is evolving (the Data (Use and Access) Act 2025). Review agreements and privacy documents against the current position.

When you are the processor

A business that handles personal data for its clients, for example a bookkeeper or payroll provider, must itself give the controller an adequate DPA. Offer a clear, short document and keep it up to date.

What to do when a supplier will not negotiate

Large software providers rarely change their standard terms for a small customer. In that case, check that the standard DPA covers the required points, record the review, and consider whether the supplier is an acceptable risk. If a critical point is missing, ask the supplier for a written confirmation, or choose a different supplier when the contract next renews.

How MTM can help

0161 835 2080
client@mtmlp.co.uk

We review supplier contracts for data protection terms, prepare data processing agreements for practices that act as processors, and update privacy documents. Data protection compliance advice, such as impact assessments, stays with your client or their data protection adviser.