Policy

UK GDPR Data Protection Policy

Effective Date: May 2026 | Next review due: May 2027

This policy explains how Mother Technologies handles personal data, both for its own business and when providing hosting and managed services to clients.

About Mother Technologies

Mother Technologies is a Managed Service Provider (MSP), providing private cloud hosting and managed services to clients across Scotland and beyond. Our hosted services reside in Tier 2, ISO27001 certified datacentres in Edinburgh, Glasgow, Dundee and Aberdeen. The datacentres are owned and managed by Neos Networks, a division of the SSE Group, and connected via the UK's biggest B2B network, designed specifically for UK critical national infrastructure.

We act in two distinct roles under UK GDPR:

- **Data Controller** — for data relating to our own business operations, staff, and suppliers.
- **Data Processor** - for client data stored, managed, or otherwise processed within our infrastructure, including as part of managed service provision (such as hosting, maintenance, backup, and related support services), processed solely under documented instructions from the controller.

In both roles, protecting data is a fundamental responsibility we take seriously.

UK GDPR and Brexit — What Applies to Us

Although the UK left the European Union, data protection law did not change in substance. The EU GDPR was incorporated into UK law as the UK General Data Protection Regulation (UK GDPR), sitting alongside the Data Protection Act 2018. The rules are substantively equivalent.

As a UK-based company processing personal data, Mother Technologies is fully subject to UK GDPR and is registered with the UK Information Commissioner's Office (ICO), the UK's independent authority for data protection regulation. Our primary data centres are located in Scotland (UK), meaning personal data is ordinarily stored within the United Kingdom.

In certain circumstances, personal data may be transferred outside the UK, for example where we use third-party service providers for backup, resilience, or infrastructure support. Where such transfers occur, we ensure they are carried out in compliance with UK GDPR requirements. Further details are set out in Section 4.

1. Who to Contact

Mother Technologies is not required to appoint a statutory Data Protection Officer under Article 37 UK GDPR.This is because we do not carry out large-scale systematic monitoring of individuals or large-scale processing of special category data as a core activity. We have instead appointed a designated Data Protection Contact responsible for overseeing compliance, handling data subject requests, and acting as the point of contact with the ICO.

Our designated Data Protection Contact is responsible for overseeing compliance with this policy and handling data-related requests.

- Email: compliance@mother.uk.net
- ICO Registration Reference: ZA804318
- ICO website: https://ico.org.uk | ICO helpline: 0303 123 1113

If you have a concern about how we handle your data and are not satisfied with our response, you have the right to complain to the Information Commissioner's Office (ICO) at any time.

2. What Data We Collect

2.1 For our own business operations (Data Controller):

- Client and supplier contact details — names, email addresses, phone numbers
- Account and billing information
- Technical data — IP addresses, system access logs
- Staff and employment records

2.2. For client data we host or process (Data Processor):

Mother Technologies provides data centre colocation, hosted services, and managed IT to a wide range of clients, including those in legal, financial, professional services, charitable, educational, and other sectors. Data belonging to clients is processed strictly in accordance with:

- The client's instructions
- A Data Processing Agreement (DPA)
- UK GDPR obligations applicable to data processors

We never access, use, or share client data for our own purposes. Clients always retain full ownership and control of their data.

3. Why We Collect Data — Lawful Basis – Specifically as a Data Controller

We only collect and use data where we have a lawful basis to do so under UK GDPR. Our primary lawful bases are:

- Contract — processing is necessary to deliver our IT and hosting services, manage billing, and fulfil our contractual obligations to clients and suppliers.
- Legitimate Interests — for security monitoring, fraud prevention, and maintaining the integrity of our systems and infrastructure, where this does not override individuals' rights.
- Legal Obligation — where we are required to retain or process data to comply with applicable laws and regulations.

We do not use data for purposes beyond what it was originally collected for, and we never sell personal data to third parties.

Where we act as a data processor, lawful bases are determined by the data controller, and we process data solely in accordance with their instructions.

4. Where Your Data is Stored

Mother Technologies acts as a data controller for personal data relating to its own business operations (such as client contacts, suppliers, and marketing communications) and as a data processor when providing hosted or managed services to clients under contract.

Personal data processed or hosted by Mother Technologies is stored primarily within our Scottish data centres, located in Edinburgh, Glasgow, Dundee, and Aberdeen, all within the United Kingdom.

In certain circumstances, including the use of trusted third-party providers for backup, resilience, support services, or other managed service components, personal data may be transferred outside the UK. Any such transfers are strictly controlled and carried out in compliance with UK GDPR.

Transfers may take place to jurisdictions recognised as providing an adequate level of data protection, such as the European Economic Area (EEA), Switzerland, New Zealand, Japan, Canada (commercial organisations), and certain UK Crown Dependencies (including Jersey, Guernsey, and the Isle of Man), allowing personal data to flow without additional safeguards under GDPR. Where transfers to non-adequate countries are necessary, appropriate safeguards under GDPR are implemented, alongside appropriate technical and organisational measures.

5. How We Protect Your Data

Our private cloud hosted services reside in Tier 2, ISO 27001 certified datacentres, owned and managed by Neos Networks, a division of the SSE Group. Neos Networks provide the UK's biggest B2B-only network designed to connect UK critical national infrastructure.

Comprehensive technical and organisational security includes:

- Physical security: Steel palisade perimeter fencing, full access control and secured perimeters, CCTV monitoring, alarmed 24/7.
- Power resilience: Dual 40kVA AC 220V UPS systems backed by a 135kW standby diesel generator.
- Cooling: N+1 dual air handling unit/condenser system.
- Fire protection: Fire detection and alarm systems, Argon gaseous fire suppression.
- Network security: Cisco firewalling with 24-hour monitoring and proactive management.
- Virtualisation: Our server estate runs on VMware's vSphere for hardware independence and portability.
- 2 Stage Backups: 1st stage daily backups replicate all virtual machines to alternative Storage Array Networks (SANs) with 14-day retention. 2nd Stage backups copy and encrypt virtual machines off-site for disaster recovery purposes with 30-day retention.
- Endpoint Detection and Response protection is enforced on our server estate and strongly encouraged on client systems.
- Access control — role-based, restricted access to systems and data with multi-factor authentication
- Organisational measures — formal data protection policies, documented procedures, role-based access control, and ongoing staff training and awareness.

No data is shared informally or outside of secure, authorised channels.

6. Sharing Data

We do not sell personal data, nor do we share it with third parties for marketing, advertising, or other commercial purposes. Personal data is only shared where required by law, with trusted service providers acting under appropriate contractual safeguards, or where explicitly instructed under a Data Processing Agreement (DPA).

7. How Long We Keep Data

We keep personal data only for as long as necessary for the purposes for which it is processed, whether acting as a data controller or a data processor under GDPR. Our standard retention periods are:

- Financial and contract records — 7 years, in line with HMRC requirements
- Staff and employment records — duration of employment plus 7 years
- Client data — retained in accordance with the client's instructions and the applicable Data Processing Agreement (DPA). Where no specific instruction is provided, a standard transition period of up to 12 months may apply
- System and security logs — retained for a period appropriate to our security monitoring obligations, typically 12 months

8. Your Rights

Under UK GDPR, individuals whose data we hold have the following rights:

- Right of access — request a copy of the data we hold about you
- Right to rectification — ask us to correct inaccurate or incomplete data
- Right to erasure — ask us to delete your data where we have no lawful reason to keep it
- Right to object — object to how we are using your data
- Right to restriction — ask us to limit processing in certain circumstances
- Right to data portability — receive your data in a structured, machine-readable format
- Right to withdraw consent — where consent is the basis for processing, you may withdraw it at any time
- Right to complain to the ICO — if you are unhappy with how we have handled your data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at any time. You can contact the ICO at ico.org.uk or on 0303 123 1113.

To exercise any of these rights, reach out to our Data Protection Contact at compliance@mother.uk.net

9. Data Breach Procedure

Mother Technologies has a documented data breach procedure which is followed in the event of a suspected or confirmed personal data breach. In such cases, we take appropriate steps in line with the relevant procedure to contain and assess the incident.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, we will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. Affected clients and/or individuals will also be informed where necessary.

All personal data breaches, whether reportable or not, are recorded in our internal breach log.

Where Mother Technologies acts as a data processor, we provide advisory support and assist with containment, assessment, and recommended next steps. However, the client remains responsible for all final decisions, including notification to the ICO.

Where we act as a data controller, we are responsible for managing the breach, including decision-making and any required regulatory reporting obligations under GDPR.

Further operational details are contained within our data breach management procedure.

10. Subject Access Requests

Any individual has the right to request a copy of the personal data we hold about them (a Subject Access Request, or SAR). To make a SAR:

- Get in touch with our Data Protection Contact at compliance@mother.uk.net
- We will verify your identity before releasing any information
- We will respond within one calendar month
- There is no charge for a SAR in most circumstances
- We will not disclose data that would infringe on the rights of other individuals, or that we are legally required to withhold.

11. Staff Training

All Mother Technologies staff who handle personal data receive training on data protection as part of their induction and on an ongoing basis. Training covers:

- Our legal obligations under UK GDPR and the Data Protection Act 2018
- How to keep data secure, including physical and digital security
- How to identify and report a data breach

Staff are supported to raise concerns without fear of blame in the case of accidental incidents.

12. The UK GDPR Principles We Follow

Everything we do with data is guided by the seven principles of UK GDPR:

- Lawfulness, fairness and transparency — we have a lawful basis and are open about how we use data
- Purpose limitation — data is only used for the reason it was collected
- Data minimisation — we only collect what we genuinely need
- Accuracy — we keep data up to date
- Storage limitation — we do not keep data longer than necessary
- Integrity and confidentiality — we keep data secure using appropriate technical and organisational measures
- Accountability — we take responsibility for our data practices and can demonstrate compliance

13. Policy Review

This policy will be reviewed annually , or sooner if there are significant changes to our business operations, the law, or guidance from the ICO. The Data Protection contact is responsible for ensuring the review takes place and that any updates are communicated to all staff. Where we make any material changes to the way we process personal data, we will notify affected individuals directly by email where possible and update this policy accordingly. This policy is made available to clients and other data subjects on our website and is provided to staff as part of induction and ongoing training.