GDPR Compliance - Privacy Notice

GDPR Privacy Notice - Viamed Group of Companies

Last Updated: March 2025

1. Introduction

This Privacy Notice explains how Viamed Group of Companies ("we", "us", "our") collects, processes, stores, and protects personal data in compliance with UK GDPR and other relevant data protection laws.

We are committed to ensuring that all personal data is handled securely, transparently, and in a way that upholds individuals' rights.

2. Who We Are

Viamed Group of Companies includes:

- Viamed Ltd
- Vandagraph Ltd
- Vandagraph Sensor Technology Ltd
- Viamed Properties Ltd

Registered Address: 15 Station Road, Cross Hills, Keighley, BD20 7DT, UK

Contact Email: dataprotectionofficer@viamed.co.uk

Telephone: +44 (0)1535 634542

Data Protection Officer (DPO): Helen Lamb

3. What Personal Data We Collect

We may collect and process the following types of personal data:

- Identity Data: Full name, job title, employer details

- Contact Data: Phone numbers, email addresses, postal addresses

- Financial Data: Bank details (for supplier and payment processing), invoice history

- Transaction Data: Records of sales, orders, and service history

- Marketing Preferences: Opt-in/opt-out records, communication preferences

- Technical Data: IP addresses, device identifiers, website usage logs (for security)

- CCTV Footage: If visiting our premises, recorded for security purposes

4. How We Collect Personal Data

We collect personal data in the following ways:

- Directly from you (e.g., when you provide contact details for services)

- Through our website (contact forms, order processing, cookies, analytics)

- From third parties (e.g., business partners, publicly available sources)

- From internal records (e.g., account transactions, contracts, invoices)

5. Purpose and Lawful Basis for Processing

We only process personal data when we have a lawful basis under UK GDPR, such as:

| Purpose of Processing | Lawful Basis |

|---|---|

| Providing products and services | Contractual necessity |

| Processing payments and invoices | Legal obligation (HMRC compliance) |

| Customer support and service management | Legitimate interest |

| Employee and supplier record-keeping | Legal obligation |

| Marketing communications (where opted-in) | Consent |

| Website analytics and security | Legitimate interest |

| Complying with regulatory requirements | Legal obligation |

| CCTV surveillance for security | Legitimate interest |

6. How We Store and Protect Data

We implement strict security measures to protect personal data, including:

- Encryption for sensitive data
- Access controls (restricted to authorized personnel)
- Regular security audits and staff training
- Firewalls and intrusion detection to prevent unauthorized access
- Secure physical storage for paper records

7. How Long We Keep Personal Data (Retention Policy)

We retain personal data only as long as necessary, following UK GDPR principles:

Data Type	Retention Period	Reason
Customer data (active)	While account is active	Service provision
Customer data (inactive)	7 years after last transaction	HMRC compliance
Employee records	6 years after employment ends	Employment law
Payroll & tax records	6 years	HMRC legal requirement
Supplier contracts	7 years after termination	Contractual audits
Marketing data	2 years after last contact	ICO guidance
CCTV footage	30 days unless part of an investigation	Security compliance
Health & safety records	3 years	Compliance requirement
Financial records	6 years	HMRC tax laws
Unsuccessful job applications	6 months	ICO best practice
Customer complaints & service logs	3 years	Dispute resolution

8. Sharing Personal Data

We do not sell personal data. However, we may share it with:

- Regulatory authorities (HMRC, ICO, UK government agencies)

- Service providers (IT support, payment processors, accountants)

- Law enforcement (if legally required)

- Auditors (for compliance and business reviews)

All third parties must comply with UK GDPR and sign Data Processing Agreements (DPAs).

9. International Data Transfers

If we transfer data outside the UK, we ensure appropriate safeguards, such as:

- UK GDPR Standard Contractual Clauses (SCCs)

- ICO-approved data protection frameworks

10. Your Rights Under UK GDPR

You have the right to:

- Access your personal data (Subject Access Request - SAR)

- Rectify inaccurate or incomplete data

- Request deletion (Right to Erasure, "Right to be Forgotten")

- Restrict processing (in certain circumstances)

- Object to processing, including marketing opt-outs

- Request data portability (to move data to another service)

- Not be subject to automated decisions (if applicable)

- Complain to the ICO if your rights are violated

How to Exercise Your Rights:

Email: dataprotectionofficer@viamed.co.uk

Phone: +44 (0)1535 634542

Address: 15 Station Road, Cross Hills, Keighley, BD20 7DT

11. Data Breaches and Incident Reporting

If a personal data breach occurs, we will:

- Assess the risk within 72 hours

- Report serious breaches to the ICO

- Notify affected individuals if necessary

- Take corrective actions to prevent future incidents

12. Updates to This Privacy Notice

We review this policy annually and update it as needed. The latest version is always available on our website.

Viamed Group of Companies

Committed to GDPR Compliance and Data Protection