Viamed Ltd GDPR Data Handling and Request Procedures

1. Purpose

This document defines the internal procedures for handling personal data and responding to data subject requests in accordance with UK GDPR.

It ensures requests are handled consistently, legal timeframes are met, and decisions are documented.

2. Scope

Applies to:

- Viamed Ltd

All staff handling personal data.

3. Responsibilities

Data Protection Officer (DPO): Oversight and decision making

Directors / Management: Support legal decisions

Staff: Identify and report requests immediately

4. Systems Containing Personal Data

- Intrastats: CRM, customer, supplier, sales

- Xero: Financial data

- Email: Communications

- File storage: HR and compliance

- Paper records

5. General Rules

- Log immediately

- Acknowledge within 5 working days

- Complete within 1 month

- Verify identity before release

6. Subject Access Requests

- Check Intrastats, Xero, Email, Files

- Extract data

- Remove 3rd party data

- Provide structured response

7. Right to Rectification

- Verify request

- Update all systems

- Notify third parties

- Restrict processing if accuracy disputed

8. Right to Restrict Processing

- Mark data as restricted

- Prevent editing/sharing

- Only allow legal use

- Inform before lifting

9. Right to Object

- Stop marketing immediately

- Assess legitimate interest

- DPO decision required

- Provide justification if refused

10. Data Breach Procedure

- Report immediately

- Record incident

- Risk assess

- Notify ICO within 72 hours if required

- Inform individuals if high risk

11. Data Handling Rules

- Access only required data

- Do not share without approval

- Use secure systems

- Report issues immediately

12. Compliance Statements

- ROPA maintained

- DPIAs conducted where required

- No automated decision making unless documented

13. Training

- Staff training required

- Refresher training periodic

14. Review

- Annual review

- Update after incidents or regulation changes