Neocare – GDPR Privacy Policy

(UK GDPR & Data Protection Act 2018)

Effective Date: November 2025

Review Date: November 2026

1. Introduction

Neocare ("we", "us", "our") is committed to protecting the privacy and personal data of our clients, customers, suppliers, and anyone who interacts with our business.

This Privacy Policy explains how we collect, use, store, share, and protect personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. What Personal Data We Collect

We may collect the following types of personal data depending on your relationship with us:

- Name, address, email, telephone number
- Organisation, job title or professional contact details
- Enquiry and communication records
- Service or product-related information
- Health information where required for care-related services
- Financial or billing information
- Technical data (e.g., IP address, website usage)

Some information may be special category data, which receives additional legal protection.

3. How We Collect Personal Data

We collect data in several ways:

- When you contact us by phone, email, website or in person
- When you request information, quotations or services
- When we provide care, products or support
- When you visit our website

- From third parties such as healthcare professionals, commissioners or suppliers (where lawful)

4. How We Use Personal Data

We use personal data to:

- Respond to enquiries and provide quotations
- Deliver products, services or care
- Maintain accurate records
- Communicate with clients, partners and professionals
- Manage accounts, billing and administration
- Meet legal, regulatory and safeguarding obligations
- Improve our services and operations
- Ensure the security and performance of our systems

We do not use personal data for unrelated marketing without consent.

5. Lawful Bases for Processing

We process personal data under one or more of the following lawful bases:

- Contract – to provide products or services you have requested
- Legal obligation – to meet regulatory or statutory requirements
- Legitimate interests – to operate and improve our business
- Vital interests – to protect life in emergencies
- Consent – where required (e.g., optional marketing)
- Public task – where applicable in regulated care settings

Special category data is processed under Article 9 UK GDPR, including for health and social care purposes.

6. Sharing Personal Data

We may share personal data with:

- Healthcare professionals or commissioners (where relevant)
- Local authorities, NHS bodies or regulatory organisations
- Trusted service providers (e.g., IT, secure storage, payment processors)
- Emergency services where necessary

- Professional advisers (e.g., legal or financial)

All third parties must comply with strict confidentiality and data protection standards.

We do not sell personal data.

7. Data Security

We take appropriate technical and organisational measures to protect personal data, including:

- Secure IT systems and access controls
- Encryption where appropriate
- Secure storage of paper records
- Staff training on confidentiality and data protection
- Regular review of security measures and procedures

8. Data Retention

We keep personal data only for as long as necessary to:

- Provide services
- Meet legal and regulatory requirements
- Resolve queries or disputes
- Maintain business records

When data is no longer required, it is securely deleted or destroyed.

9. Your Rights

Under UK GDPR, you have the right to:

- Be informed about how your data is used
- Access your personal data
- Request correction of inaccurate information
- Request deletion in certain circumstances
- Restrict or object to processing
- Request data portability
- Withdraw consent (where consent is the lawful basis)
- Complain to the Information Commissioner's Office (ICO)

We normally respond to requests within one month.

10. Subject Access Requests

You can request a copy of the personal data we hold about you.

We may ask for proof of identity to protect your information.

There is usually no fee unless the request is excessive or repeated.

11. Data Breaches

If a personal data breach occurs, we will:

- Assess the risk
- Notify the ICO within 72 hours where required
- Inform affected individuals without undue delay if there is a high risk to their rights or freedoms

12. International Transfers

We do not transfer personal data outside the UK unless appropriate safeguards are in place, such as:

- Adequacy regulations
- Standard contractual clauses
- Equivalent protection measures