



Privacy Policy

Remote Care Administration Solutions

This Privacy Policy explains how Deskbridge collects, uses, stores, and protects personal data. It applies to data collected through the Deskbridge website (deskbridge.co.uk) and to data processed on behalf of our clients in the course of delivering remote administrative support services.

Document Detail	Information
Document	Privacy Policy
Version	1.0
Last Updated	May 2026
Data Controller	Deskbridge
Contact	hello@deskbridge.co.uk
Telephone	0113 322 6376
Supervisory Authority	Information Commissioner's Office (ICO)

1. Who We Are

Deskbridge is a remote care administration service providing dedicated administrative staff to health and social care providers across the United Kingdom. Our operational staff are based in Nairobi, Kenya, and are directly employed, trained, and supervised by Deskbridge.

For data collected through our website (such as contact form submissions), Deskbridge acts as the **Data Controller** — meaning we determine the purposes and means of processing that data.

For data we access and process on behalf of our clients (such as staff records, service user information, and compliance documentation), Deskbridge acts as a **Data Processor** — meaning we process data only on the instructions of the client, who remains the Data Controller.

Our contact details for data protection enquiries are:

- Email: hello@deskbridge.co.uk
- Telephone: 0113 322 6376
- Website: deskbridge.co.uk

2. What Data We Collect

2.1 Data collected directly through our website

When you use the Deskbridge website, we may collect the following personal data:

- Full name
- Email address
- Telephone number
- Organisation name
- Care setting type
- Details of your administrative needs (as provided in the contact form)
- Technical data such as IP address, browser type, and device information (collected automatically through cookies and analytics tools, where applicable)

2.2 Data processed on behalf of our clients

In the course of delivering our services, Deskbridge staff may access and process the following categories of data on behalf of our clients:

- Staff records — names, contact details, employment documents, DBS information, right-to-work documents, references, training records, supervision notes, and appraisal records
- Service user information — names, care plan references, referral documentation, assessment records, and support plan identifiers
- Financial data — invoice details, timesheet records, payment records, and supplier information
- Recruitment data — candidate names, contact details, application information, interview records, and onboarding documentation
- Communication records — emails, call logs, and correspondence handled on behalf of the client

Deskbridge handles administrative elements of these records only and does not make clinical or care judgements. The specific data categories processed for each client are documented in the Service Schedule and Data Processing Agreement agreed during onboarding.

3. Why We Collect and Process Data

3.1 Website data

Purpose	Legal Basis (UK GDPR)
Responding to contact form enquiries	Legitimate interest (responding to a business enquiry)
Following up with prospective clients	Legitimate interest (business development)
Improving our website and services	Legitimate interest (service improvement)
Complying with legal obligations	Legal obligation

3.2 Client data

Data processed on behalf of our clients is processed on the legal basis of **contractual necessity** — it is necessary for us to access and process this data in order to deliver the administrative services agreed under our Terms of Service. The client, as Data Controller, is responsible for ensuring that their own legal basis for collecting and holding the data is valid.

4. Where Data Is Processed

Deskbridge's administrative staff are based in **Nairobi, Kenya**. This means that personal data accessed by our staff in the course of delivering services to UK care providers is processed outside of the United Kingdom.

Kenya is not currently subject to a UK adequacy decision under UK GDPR. To ensure that international data transfers are lawful and that personal data receives an equivalent level of protection, Deskbridge implements the following safeguards:

- Standard Contractual Clauses (SCCs) as approved under UK data protection law, incorporated into the Data Processing Agreement with each client
- Strict access controls — staff access only the systems and data necessary for their assigned tasks
- Encrypted connections between Deskbridge staff and client systems at all times
- Individual, role-based authentication — no shared logins or generic accounts
- Mandatory data protection training for all staff as part of their induction programme
- Prohibition on downloading, copying, or storing client data on personal devices or local storage
- Immediate revocation of all access upon termination of the client relationship or staff departure

Full details of the technical and organisational measures in place are documented in the Data Processing Agreement provided to each client.

5. How Long We Keep Data

Data Type	Retention Period
Contact form enquiries (website)	12 months from submission, then securely deleted
Prospective client communication	12 months from last contact, then securely deleted

Client service data (processed on behalf of clients)	Retained for the duration of the service agreement only. Securely deleted within 30 days of contract termination
Invoices and financial records	6 years from the date of the transaction, as required by HMRC
Deskbridge internal staff records	Duration of employment plus 2 years

6. Who We Share Data With

Deskbridge does not sell, rent, or trade personal data to any third party.

In the course of operating our business and website, personal data may be shared with the following categories of third-party service providers:

Third Party	Purpose	Data Shared
FormCarry	Processing contact form submissions	Name, email, phone, message content
GoDaddy	Hosting the Deskbridge website	Technical and server data
Google Analytics (if enabled)	Website usage analysis	Anonymised browsing data, IP address
Payment processor (e.g. GoCardless, Stripe)	Processing client payments	Client billing information
Airtable	Internal task and client management	Client name, task data, operational records

All third-party processors are contractually required to handle data securely and in accordance with applicable data protection law.

We may also disclose personal data where required by law, regulation, or court order.

7. Data Security

Deskbridge takes appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or alteration. These measures include:

- Encrypted connections (TLS/SSL) for all data in transit
- Role-based access controls — staff access only the systems and data relevant to their assigned clients and tasks
- Individual authentication — no shared logins, passwords, or generic accounts
- Mandatory data protection and confidentiality training for all Deskbridge staff during induction
- Regular review of access permissions, with immediate revocation upon staff departure or client termination
- Prohibition on storing client data on personal devices, USB drives, or unencrypted local storage
- Secure deletion of all client data within 30 days of contract termination

While we take all reasonable precautions, no method of electronic transmission or storage is 100% secure. In the unlikely event of a data breach, Deskbridge will notify the affected client and, where required, the Information Commissioner's Office within 72 hours of becoming aware of the breach.

8. Your Rights

Under the UK General Data Protection Regulation, you have the following rights in relation to your personal data:

Right of access: You may request a copy of the personal data we hold about you.

Right to rectification: You may request that we correct any inaccurate or incomplete data.

Right to erasure: You may request that we delete your personal data, subject to any legal obligations requiring us to retain it.

Right to restrict processing: You may request that we limit how we use your data in certain circumstances.

Right to data portability: You may request that we provide your data in a structured, machine-readable format.

Right to object: You may object to the processing of your data where it is based on legitimate interest.

Right to withdraw consent: Where processing is based on consent, you may withdraw that consent at any time.

To exercise any of these rights, please contact us at hello@deskbridge.co.uk or by telephoning 0113 322 6376. We will respond to your request within 30 days.

Note for care provider clients: If you are a service user, staff member, or other individual whose data is processed by Deskbridge on behalf of a care provider, your rights should be exercised by contacting the care provider directly (as the Data Controller). Deskbridge will assist the care provider in responding to such requests as required under our Data Processing Agreement.

9. Cookies

The Deskbridge website may use cookies — small text files placed on your device — to improve your browsing experience and to help us understand how visitors use our site.

9.1 Types of cookies we may use:

Cookie Type	Purpose	Duration
Essential cookies	Required for the website to function correctly	Session
Analytics cookies	Help us understand how visitors use the site	Up to 2 years

You can control and delete cookies through your browser settings. Disabling cookies may affect the functionality of certain features on our website.

10. Children's Data

The Deskbridge website and services are directed at businesses and professionals. We do not knowingly collect personal data from individuals under the age of 18 through our website. If you believe we have inadvertently collected data from a minor, please contact us immediately at hello@deskbridge.co.uk and we will delete it.

11. Complaints

If you are dissatisfied with how Deskbridge has handled your personal data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

- Website: ico.org.uk
- Telephone: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

We would appreciate the opportunity to address your concerns before you contact the ICO. Please contact us at hello@deskbridge.co.uk in the first instance.

12. Changes to This Policy

Deskbridge may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or operational processes. The updated policy will be published on our website at deskbridge.co.uk with the revised date shown at the top of the document.

Where changes are material — particularly any changes to how or where data is processed — we will notify existing clients in writing.

13. Governing Law

This Privacy Policy is governed by the laws of England and Wales and is subject to the jurisdiction of the courts of England and Wales.

This Privacy Policy should be published on the Deskbridge website under the 'Privacy Policy' footer link and provided to clients during onboarding alongside the Terms of Service and Data Processing Agreement.

This document does not require a signature. It is a public-facing policy document.