

CLOSEDAY LTD

PRIVACY NOTICE

Effective from: February 1, 2026

Summary

This Privacy Notice explains how Closeday Ltd ("Closeday", "we", "us") collects, uses, and protects personal data. We provide corporate insolvency services.

Key points:

- We collect data to provide insolvency services and operate our platform
- Your rights depend on your relationship with us—whether you are an outbound marketing recipient, website visitor, registered user, customer, or case stakeholder
- Case stakeholders (such as creditors, employees, shareholders, landlords, and former employees) may receive communications from us that are legally required and from which you cannot opt out
- We retain data for periods required by law (up to 6 years for insolvency cases)
- You can contact us at privacy@closeday.com with questions or requests

1. Who We Are

Summary: Closeday Ltd is a corporate insolvency practice. Our role as data controller or processor depends on your relationship with us.

Closeday Ltd is registered in England and Wales (Company No. 16740724). Our registered address is Suite RA01, 195-197 Wood Street, London, E17 3NU, United Kingdom.

We are authorised by the Institute of Chartered Accountants in England and Wales (ICAEW) to act as an insolvency practitioner firm.

For data protection purposes, Closeday Ltd is the "data controller" for personal data we collect directly, except where:

1. Non-customer users share personal data via their user account, in which case the user is the data controller and we act as processor; or
2. Customer companies share personal data in phases prior to appointment, where the company engaging us acts as controller and we act as processor (see Section 4 below).

Contact for data protection matters: privacy@closeday.com

2. About This Notice

Summary: This notice applies to everyone whose data we control or process. Different sections are relevant depending on your relationship with us.

This Privacy Notice applies to:

- **Outbound marketing recipients** who we contact about our services
- **Website visitors and anonymous users** who browse or use our online tools without creating an account
- **Registered users** who create an account on our platform
- **Customers** (company directors) who engage our insolvency services
- **Case stakeholders** including creditors, employees, former employees, shareholders, landlords, and other parties affected by an insolvency case we administer

We have organised this notice so you can easily find the section relevant to you. The legal basis for our processing and your rights may differ depending on your category.

If you are a creditor, employee, shareholder, or other stakeholder in an insolvency case, you may receive communications from us that are legally required. You cannot opt out of these statutory communications, though you can opt out of marketing.

3. What Data We Collect

Summary: We collect different types of data depending on how you interact with us. The categories below are illustrative and not exhaustive.

3.1 Data from Website Visitors and Anonymous Users

When you visit our website or use our online tools without creating an account, we collect technical data (such as IP address, browser type, and device information), usage data (such as pages visited), cookie data (see our Cookie Policy), and any information you choose to provide.

You should not submit detailed third-party personal data (information about other individuals) without first creating an account.

3.2 Data from Registered Users

When you create an account, we collect data you provide, account credentials, and data necessary to operate your account.

We may also collect identification documents and information about you and relevant third parties (such as other directors or beneficial owners) to the extent needed to complete anti-money laundering checks and establish a business relationship. This may occur before you become a customer.

3.3 Data from Customers

When you engage our services, we collect information necessary for insolvency proceedings. This includes company financial information, books and records, contracts, information about directors and stakeholders, banking details, information relating to director conduct, and any other information relevant to the case.

3.4 Data About Case Stakeholders

During an insolvency case, we receive and process data about various parties such as creditors, employees, former employees, shareholders, debtors, directors, landlords, suppliers, professional advisers, and other parties relevant to the case.

3.5 Data About Job Applicants

During recruitment processes, we collect candidate information including details you provide in your application, including your CV or resume, cover letter, contact details, employment history, educational background, and professional qualifications. We may also collect references from previous employers, information from publicly available professional profiles, and records of our communications with you during the recruitment process.

Where relevant to the role, we may collect right-to-work documentation and, for certain positions, conduct background checks in accordance with applicable law. We will inform you before conducting any such checks.

3.6 Special Category Data

We may collect special category data (sensitive personal data) in certain circumstances.

For AML/KYC compliance, we may collect information relating to criminal records or allegations as part of our anti-money laundering and know-your-customer procedures. This

applies to directors, beneficial owners, and other controlling persons, and may occur at the registered user stage before any customer relationship.

During insolvency cases, we may receive sensitive data where relevant—for example, employee health information affecting pay calculations, or information relevant to investigating director conduct. We only process special category data where strictly necessary and with appropriate safeguards.

4. Controller and Processor Roles

Summary: Our role changes depending on the stage of your journey with us. Sometimes we control the data; sometimes you do.

Stage	Who Controls the Data	Closeday's Role
Candidates	Closeday	Controller
Outbound marketing recipients	Closeday	Controller
Website visitors and anonymous users	Closeday	Controller
Registered user (pre-engagement)	You (the user) for data you provide	Processor
Customer engagement (pre-appointment)	The company engaging us	Processor
Post-appointment (insolvency case)	Closeday	Controller

What this means for you:

As an outbound recipient, website visitor, or anonymous user: We control your data under this Privacy Notice.

As a registered user: When you create an account, you become the data controller for personal data you submit through the Platform. We process it on your behalf as your data processor. Individuals whose data you share should direct any data subject requests to you, not us.

As a customer (pre-appointment): When your company engages us, the company is the data controller. We process data on your behalf. Individuals whose data you share should direct data subject requests to you or the company, not us. Our processing is governed by the Data Processing Agreement in your Customer Terms.

Post-appointment: Once an insolvency practitioner is appointed, Closeday becomes the data controller for all case-related personal data under statutory authority.

5. Why We Process Data and Our Legal Bases

Summary: We process data for specific purposes, each with a legal basis under UK GDPR.

5.1 Candidates

We process data from job applicants for purposes including evaluating your application, communicating with you about the recruitment process, conducting interviews and assessments, verifying your qualifications and references, conducting background and right-to-work checks where applicable, and maintaining records of our recruitment decisions.

If you are unsuccessful, we may retain your data to consider you for future opportunities. You can ask us to delete your data at any time if you do not wish to be considered for other roles.

Legal basis: Legitimate interest (evaluating candidates and making hiring decisions); Legal obligation (right-to-work checks under Immigration, Asylum and Nationality Act 2006); Consent (for contacting references and retaining data for future opportunities).

5.2 Outbound Recipients, Website Visitors, and Anonymous Users

We process data from outbound marketing recipients, website visitors, and anonymous users for purposes including operating and securing our website, providing online tools, analysing usage to improve our services, and contacting prospective customers about our services. You can opt out of marketing communications at any time by clicking "unsubscribe" in any email, adjusting your account settings, or emailing privacy@closeday.com.

Legal basis: Legitimate interest.

We rely on legitimate interest for this processing, including marketing communications. We have conducted a Legitimate Interest Assessment which concluded:

Purpose: To enable prospective customers to explore our services and make informed decisions, and to inform relevant business professionals about services that may benefit them or their clients.

Necessity: Processing is necessary because users reasonably expect to use online tools to research insolvency options, requiring signup before any interaction could deter users who need time to consider their options, and business professionals benefit from learning about specialist services relevant to their work.

Balancing test: We have balanced our interests against individuals' rights and freedoms. We collect minimal data at these stages, restrict third-party personal data collection for anonymous users, retain data for a limited period (12 months) then delete it, and provide easy opt-out mechanisms. The processing does not involve sensitive data (except where required for AML/KYC at later stages). There is no significant imbalance of power—these are business professionals making commercial decisions.

Conclusion: Our legitimate interest in providing accessible services and informing relevant professionals outweighs the minimal privacy impact, given the safeguards in place.

5.3 Registered Users

We process data from registered users for purposes including providing and maintaining your account, processing data you submit, sending service-related communications, and conducting anti-money laundering and identity verification checks.

Legal basis: Contract (User Terms) for account operation; Legal obligation (MLR 2017) for AML/KYC checks.

When you submit data about third parties, you are the controller and we process as your processor.

5.4 Customers (Pre-Appointment)

We process data from customers for purposes including providing insolvency advisory services, processing data on behalf of your company, and preparing for potential appointment.

Legal basis: Contract.

5.5 Post-Appointment (Insolvency Cases)

We process data in insolvency cases for purposes including administering the estate, corresponding with stakeholders, statutory reporting, investigating company affairs and director conduct, distributing assets and dividends, and maintaining case records.

Legal basis: Legal obligation (Insolvency Act 1986, Insolvency Rules, and related legislation).

Beyond statutory duties, we have legitimate interests in maintaining comprehensive records, defending potential claims, and professional regulatory compliance. These interests are balanced against stakeholder rights through limited retention periods, security measures, and prompt responses to data subject requests.

6. Information for Case Stakeholders

Summary: If you are a creditor, employee, former employee, shareholder, landlord, or other party in an insolvency case we administer, this section explains how we handle your data.

6.1 How We May Receive Your Data

We may receive your personal data from directors, creditors, or other stakeholders; the company's records; publicly available sources (e.g., Companies House); directly from you (e.g., claim forms); professional advisers, vendors, and suppliers; and private or proprietary sources.

6.2 Why We Process Your Data

We process your data to notify you of the insolvency and your rights, adjudicate claims, distribute dividends, investigate company affairs, fulfil statutory reporting requirements, respond to your enquiries, and fulfil our duties under our business undertakings. This list is not exhaustive.

6.3 Legal Basis

Our processing is based on legal obligation (Insolvency Act 1986, Insolvency Rules) and legitimate interest (proper administration of the estate, defending claims, maintaining records).

6.4 Your Rights as a Case Stakeholder

You have rights under UK GDPR (see Section 8), but some rights are limited in the insolvency context. We cannot delete data required for statutory purposes or restrict processing required by law. We will provide access to your data upon request, subject to legal privilege and confidentiality.

7. Who We Share Data With

Summary: We share data with sub-processors and third parties where necessary for our services, legal compliance, or legitimate business purposes.

We may share your data with third parties and sub-processors for purposes including regulatory compliance, statutory filings, legal proceedings, tax matters, stakeholder notifications, banking, asset realisation, IT infrastructure, insurance, and professional services.

We maintain a list of our sub-processors (third-party service providers who process data on our behalf). This is available upon request.

7.1 International Transfers

Our primary data residency is the UK and EU, which provides compliance with both UK GDPR and EU GDPR. There are no data residency requirements under insolvency law.

Some of our service providers may be located outside the UK or the EU. Where we transfer personal data internationally, we ensure appropriate safeguards are in place:

- Transfers to countries with UK adequacy decisions (including the EU)
- Standard Contractual Clauses approved by the ICO
- UK-US Data Bridge certification (for US providers in the Data Privacy Framework)

8. Your Rights

Summary: UK GDPR gives you rights over your personal data. Some rights are limited depending on our legal basis for processing.

You have the right to:

Right	Description	Limitations
Access	Request a copy of your personal data	May be limited by legal privilege or third-party rights
Rectification	Correct inaccurate data	We may need to verify corrections
Erasure	Request deletion of your data	Does not apply where we have legal obligations to retain
Restriction	Limit how we use your data	Limited where processing is legally required
Portability	Receive your data in machine-readable format	Applies only to data processed by consent or contract
Object	Object to processing based on legitimate interest	We may continue if we have compelling grounds
Withdraw consent	Where processing is based on consent	Does not affect lawfulness of prior processing

8.1 How to Exercise Your Rights

For most requests, you can manage your data directly through your account settings. If you cannot find the option you need, or if you do not have an account, contact us at privacy@closeday.com.

We will respond within one month. Complex requests may take up to three months, and we will inform you if this is the case.

We may ask you to verify your identity before processing your request.

8.2 Right to Complain

If you are not satisfied with how we handle your data, you can complain to the Information Commissioner's Office (ICO) at ico.org.uk.

9. Data Retention and Security

Summary: We keep data for as long as necessary and protect it with appropriate security measures.

#	Data Category	Retention Period	Reason
1	Anonymous user data	12 months from last activity	Allow reasonable time for users to return

2	Registered user account data	12 months from account deactivation	Allow reasonable time for users to return
3	Customer data (engaged but case not proceeding)	6 years from engagement ending or cancellation	Potential claims limitation period
4	Insolvency case records (including stakeholder personal data)	6 years from case closure	Insolvency Rules; professional obligations; potential claims
5	Job Candidate	12 months from last activity or until consent is withdrawn	Allow reasonable time for candidates to return

After the retention period, data is securely deleted or anonymised.

We protect your data through encryption, access controls, staff training, security assessments, secure cloud infrastructure, and incident response procedures. No system is completely secure. If you believe your data has been compromised, contact us immediately at privacy@closeday.com.

10. Changes to This Notice

We may update this Privacy Notice from time to time. Changes take effect when posted on our website. For significant changes, we will notify registered users by email.

The "Effective Date" at the top indicates when this notice was last updated.

11. Contact Us

For information about Closeday, visit www.closeday.com. For any questions about this Privacy Notice or how we handle your data, please email privacy@closeday.com.