Privacy Policy



Contents

Version History 2
Introduction 3
Contact Details 3
What Information We Collect 4
How We Collect Your Data 5
How We Use Your Data 5
Marketing and Opt-Out 7
Cookies 7
Change of Purpose 7
Disclosures of Your Data 7
Security 8
Data Retention 8
Your Legal Rights 8

Version History

Version	Date	Details of Amendments	Author	Approved By
1.1	19/05/2025	Document creation	J Bingham	Ilan Leshem
1.1	30/09/2025	Review no change	C Maurice	Ilan Leshem
1.2	26/08/2025	Reworded and restructured	Bilal Amir	Bradley Wood
1.3	28/10/2025	Formatted for consistency	Suchitra G	Bradley Wood
1.4	30/08/2026	Updated header with PP logo	Ilan Leshem	Bradley Wood
1.5	30/10/2026	Annual review of policy	Bradley Wood	Bradley Wood
1.6	10/22/2026	Update to incorporate MCP-specifics	J Bingham	Ilan Leshem

Introduction

Welcome to the Privacy Policy of Primary Portal Solutions Ltd ("Primary Portal", "we", "our", or "us").

We are a limited company registered in England and Wales under company number 12639845. Our registered office is at Broadley House, 48 Broadley Terrace, London, NW1 6LG, United Kingdom. We are also registered with the Information Commissioner's Office (ICO) under registration number A8775555.

This policy explains how we collect, use, disclose, and protect your personal data, and outlines your rights. It applies to visitors to our website, our clients, the individuals at our clients who use our platform and services (including our MCP Service) and individuals whose business contact details appear in the deal data we make available on the platform. Personal data included in the deal data and required for platform access consists of:

Buy-side user: first and last names, corporate email address and chosen country of jurisdiction.
Bank user: As above, without country of jurisdiction.

We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), in each case as amended, including by the Data (Use and Access) Act 2025.

This website is not intended for children, and we do not knowingly collect data relating to children.

Contact Details

We have appointed a **Data Privacy Manager** who oversees this policy and manages any questions, requests, or complaints.

Contact details:
Data Privacy Manager
Primary Portal Solutions Ltd
Broadley House, 48 Broadley Terrace
London, NW1 6LG, United Kingdom
Email: **dpo@primaryportal.com**

You have the right to make a complaint at any time to the ICO (www.ico.org.uk), the UK regulator for data protection. However, we would appreciate the opportunity to address your concerns directly before you contact the ICO. If you have a complaint about how we use your personal data, please contact us using the details above. We will acknowledge your complaint within 30 days, take appropriate steps to respond to it, and tell you the outcome without undue delay.

Changes to this policy: This policy was last updated on 10November 2026. We review it regularly and will post any changes on this page. Historic versions are available on request.

Your duty to inform us of changes: Please keep us informed if your personal data changes while we hold it.

Third-party links: Our website may include links to third-party websites or applications. Clicking these may allow third parties to collect data about you. We do not control these sites and are not responsible for their privacy practices.

What Information We Collect

Personal data means any information that identifies you. It does not include anonymous or aggregated data.

We may collect the following types of personal data:

- **Identity Data**: first name, last name, username or similar identifier.
- **Contact Data**: email address, telephone numbers.
- **Technical Data**: IP address, login data, browser type/version, time zone, location, plug-ins, operating system, and platform.
- **Usage Data**: information about how you use our website, platform, products and services, including the searches and queries you make, API and MCP tool calls, and associated timestamps, volumes, IP addresses and client identifiers.
- **Marketing and Communications Data**: preferences for receiving marketing and communications.
- **Profile Data**: your platform account details and settings, the organisation you work for, your job title, and feedback you give us.
- **Financial and Transaction Data**: billing contact and invoice details, and details of the services you or your organisation have bought from us.

We may also collect **Aggregated Data** such as usage statistics. Aggregated Data may be derived from personal data but is not considered personal data in law as it does not identify you. However, if we link Aggregated Data with personal data, we treat the combined data as personal data.

We do not collect **Special Category Data** (e.g. race, religion, health, biometrics) or information relating to criminal convictions.

If you fail to provide data: Where data is required by law or contract, we may not be able to provide services if you fail to supply it.

How We Collect Your Data

We use several methods to collect personal data:

- **Direct interactions:** When you provide information by filling in forms, corresponding by email or telephone, or when you become a client.
- **Automated technologies:** As you interact with our website, platform and MCP Service, we automatically collect Technical Data using cookies, server logs, and similar tools. See our Cookie Policy for details.
- **Third parties:** We may receive data about you from your organisation (for example, when it asks us to set up a user account for you, or when your name is included in a term sheet) and from publicly available sources.

How We Use Your Data

We will only use your data where permitted by law. Most commonly, we rely on:

- **Contract:** To perform a contract with you or to take steps at your request prior to entering into a contract. Where our contract is with your organisation rather than with you, we rely on legitimate interests instead.
- **Legitimate interests:** To operate our business effectively, provided that your rights are not overridden.
- **Legal obligation:** To comply with applicable laws.
- **Consent:** Where you have explicitly provided consent (e.g. marketing or to non-essential cookies).

We may process your data for more than one lawful ground depending on the purpose. Contact us if you need further details. Please refer to the Data Use Table below for reference.

Data Use Table

Purpose/Activity	Type of Data	Lawful Basis (including legitimate interest)
Registering you as a client	Identity, Contact	Performance of a contract
Managing our relationship (e.g. policy changes, feedback requests)	Identity, Contact, Profile, Marketing	Contract; Legal obligation; Legitimate interest (keeping records updated, studying usage trends)
Administering business and website (e.g. troubleshooting, IT, security, reporting)	Identity, Contact, Technical	Legitimate interest (running business, IT services, network security, preventing fraud, restructuring); Legal obligation
Using analytics to improve services	Technical, Usage	Legitimate interest (developing products, improving services, marketing strategy)
Providing our platform and MCP Service to your organisation, including managing user accounts and access credentials	Identity, Contact, Profile, Technical, Usage	Contract (where you are our client); legitimate interests (providing the services our clients have contracted for)
Monitoring use of our platform, and MCP Service to enforce our terms (including fair use thresholds) and protect our data	Technical, Usage	Legitimate interests (protecting our data and services, and enforcing our terms)

Billing and collecting payments	Identity, Contact, Financial and Transaction	Contract; legitimate interests (recovering debts owed to us)
Sending you marketing about our services	Identity, Contact, Profile, Usage, Marketing and Communications	Legitimate interests (developing our business); consent where PECR requires it
Making deal data available to our clients through our platform and MCP Service	Identity, Contact (business contact details and role in a transaction)	Legitimate interests (providing our clients with accurate and complete information about capital markets transactions)

Marketing and Opt-Out

We will not share your personal data with third parties for marketing without your **opt-in consent**.

You can opt out of marketing at any time by:

- Logging into your account and updating your preferences.
- Adjusting checkboxes on relevant forms.
- Using unsubscribe links in our emails.
- Contacting us directly.

Cookies

We ask for your consent before setting non-essential cookies, except where the law allows us to set them without consent (for example, certain analytics cookies, which you can opt out of). You can also configure your browser to refuse all or some cookies, or to alert you when cookies are set. Disabling cookies may cause parts of our website to not function properly. See our Cookie Policy for further details.

Change of Purpose

We will only use your personal data for the purpose for which it was collected, unless we reasonably consider another use to be compatible. If we need to use it for an unrelated purpose, we will notify you and explain the legal basis.

Disclosures of Your Data

We may share your personal data with:

- **Internal third parties:** Other entities within our group.
- **External third parties:**
  - Service providers (including IT and hosting).
  - Professional advisers (auditors, lawyers, bankers, insurers).
  - Prospective or actual buyers of, or successors to, all or part of our business.

International transfers: If we transfer your data outside the UK, we make sure it is protected by appropriate safeguards, such as UK adequacy regulations (including the UK-US data bridge) or the ICO's International Data Transfer Agreement or Addendum.

We require our service providers to keep your data secure and to process it only on our instructions. Our professional advisers, and any buyer of our business, process your data as independent controllers under their own legal obligations.

Security

We use appropriate technical and organisational measures to prevent accidental loss, unauthorised access, or disclosure of personal data.

Access is limited to individuals with a legitimate business need, who are bound by confidentiality obligations.

We maintain procedures to detect and respond to personal data breaches. Where legally required, we will notify the ICO and, where a breach is likely to result in a high risk to you, we will also notify you, without undue delay.

Data Retention

We retain personal data only for as long as necessary to meet the purposes for which it was collected, including legal, tax, and regulatory requirements.

We may extend retention where:

- Complaints are ongoing.
- We reasonably believe litigation may arise.

Retention periods are set after considering:

- The volume, nature, and sensitivity of the data.
- Risks of unauthorised disclosure or misuse.
- The purposes of processing and whether they can be achieved otherwise.
- Applicable laws and regulations.

Where data is anonymised, we may retain it indefinitely for research or statistical purposes, and to improve the performance of the platform.

Your Legal Rights

Under data protection law, you have the right to:

- **Access:** Request a copy of your personal data.
- **Correction:** Rectify inaccurate or incomplete data.
- **Erasure:** Request deletion of data in certain cases.
- **Objection:** Object to processing, including for marketing.
- **Restriction:** Request suspension of processing under certain circumstances.

- **Portability:** Request your data in a structured, machine-readable format.
- **Withdraw consent:** Withdraw consent at any time where consent is the legal basis for processing.
- **Automated decision-making:** We do not make decisions about you based solely on automated processing that have legal or similarly significant effects on you.

No fee required: You will not be charged for exercising your rights. However, if a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse to act on it.

Verification: We may request information to confirm your identity before processing requests.

Response times: We will respond within one month of receiving your request or, if we need it, the information we ask for to confirm your identity or clarify your request. We may extend this by up to two further months if your request is complex or you have made several requests and will tell you if we do. When responding to an access request, we will carry out a reasonable and proportionate search for your personal data.