KUBERNO

Privacy Policy

1. Background

Last updated 1 June 2026

1.1. This policy (Privacy Policy) tells you how we look after your personal data when you visit our website at Kuberno.com (Website) or use our proprietary software, Kube (Site), where you are a prospective or current customer of our business, where you use Kube on behalf of a customer or employer, or where you are another type of business contact, such as a supplier or service provider to our business. For certain information processed in Kube on behalf of our customers (for example, entity/contact and relationship data that customers upload or input), Kuberno acts as a processor (or sub-processor) and the relevant customer is the controller.

1.2. This policy sets out what information we collect about you, what we use it for and who we share it with. It also explains your rights under data protection laws and what to do if you have any concerns about your personal data.

1.3. We may sometimes need to update this Privacy Policy to comply with new business practices or legal requirements. You should check this Privacy Policy regularly to see whether any changes have occurred.

This Privacy Policy applies to users in the UK, the EEA and the United States. Additional disclosures may apply to you depending on where you are located and the local laws that apply.

2. Who we are and other important information

2.1 We are Kuberno Limited. We are a company registered in England and Wales with company number 12391985, whose registered address is at 3rd Floor, 86-90 Paul Street, London, EC2A 4NE. In this privacy policy, we will refer to ourselves as 'we,' 'us' or 'our.'

2.2 We are the data controller for personal data collected through our websites and services, including country-specific versions of our Website made available to users in the United States.

2.3 For all visitors to our Website and for personal data we collect directly through Kube (for example, account, billing, usage, and support information), we are the data controller of that information (which means we decide what information we collect and how it is used). Where our customers upload, create or otherwise process personal data through Kube as part of using the service, we act as a processor on behalf of that customer, who is the controller.

2.4 Our Data Protection and Privacy Manager can be contacted at privacy@kuberno.com.

2.5 We are registered with the Information Commissioner's Office (ICO), the UK regulator for data protection matters, under number ZA817997.

2.6 For the purposes of Article 27 of the EU General Data Protection Regulation, our representative in the European Union can be reached at privacy@kuberno.com. Individuals located in the EEA may contact our EU representative directly with any data protection enquiries.

3. Contact Details

3.1 If you have any questions about this Privacy Policy or how we use personal data, you can contact us using the details below.

For general queries, contact: theteam@kuberno.com

For privacy queries and to exercise your data protection rights, please contact: privacy@kuberno.com.

Or by writing to us at our registered address.

4. The information we collect about you

4.1 Personal data means any information which does (or could be used to) identify a living person. We have grouped together the types of personal data that we collect, and where we received it from.

4.2 Type of personal data: Set out below are the general categories and details of retention periods in relation to those categories and, in each case, the types of personal information that we collect, use, and hold about you. Where we process customer-provided personal data in Kube as a processor, retention is determined by our customer's instructions and the applicable customer contract, subject to any lawful requirement for us to retain certain records.

General Category	Types of Personal Data	Retention Periods (indicative)
Identity Information	This is information relating to your identity such as your name (including any previous names and any titles that you use), gender, marital status, and date of birth.	Duration of relationship + 6 years (UK limitation period)
Contact Information	This is information relating to your contact details such as email address, addresses, telephone numbers	Duration of relationship + 6 years
Account Information	This is information relating to your account with us (including username and password)	Duration of relationship + 6 years
Payment Information	This is information relating to the methods by which you provide payment to us such as bank account details and/or payment card details (processed securely by our payment service providers) and details of any payments (including amounts and dates) that are made between us.	7 years from end of accounting period (s.388 CA 2006; ML Regs 2017)

Transaction Information	This is information relating to transactions between us such as details of the goods, services and/or digital content provided to you and any returns details	7 years from end of accounting period
Survey Information	This is information that we have collected from you or that you have provided to us in respect of surveys and feedback	Until purpose fulfilled, then aggregated; max 24 months
Marketing Information	This is information relating to your marketing and communications preferences	Until opt-out, then suppression list indefinitely
Website, Device and Technical Information	This is information about your use of our website and technical data which we collect (including your IP address, the type of browser you are using and the version, the operating system you are using, details about the time zone and location settings on the device and other information we receive about your device)	14 months maximum (analytics)
Usage and Log Data (Kube)	This is information about how users access and use Kube, such as login events, usage metrics, feature interaction data, timestamps, and technical logs associated with user accounts.	Duration of account + 12 months (operational logs)
Support and Ticket Information	This is information you provide when you contact us for support (for example via email, chat, or ticketing systems), which may include the content of your request, attachments, and any information needed to investigate and resolve the issue.	12 months
Community Moderation Information	This is information generated in connection with moderation of our community (for example, reports, complaints, enforcement actions, and audit records relating to community posts or accounts), where retained.	12 months
Community Membership Information	This is information that we collect from you, or that you choose to share with us, in connection with your participation in our community. This may include information you provide when joining the community, your contributions to community discussions, feedback, opinions, comments, content you post or share, and any other personal information that you choose to make available through your activity in the community.	12 months

5. The information we receive from third parties

We may receive personal data about you from third parties, where permitted by law. This may include B2B prospecting sources and enrichment providers, publicly available registers, and professional networks (for example, business-focused social networks). Where we obtain your personal data from third parties, we will provide you with any additional information required by applicable law.

6. Cookies and similar technologies

We use cookies and similar technologies on our Website/Site to help it function, to improve performance, and to understand how it is used. Where required by law (for example in the UK/EEA), we will ask for your consent before placing non-essential cookies and provide you with tools to manage your preferences. Further information is provided in our Cookie Policy.

7. How we use your information

7.1 We are required to identify a legal justification (also known as a lawful basis) for collecting and using your personal data. There are six legal justifications which organisations can rely on. The most relevant of these to us are where we use your personal data to:

- Pursue **our legitimate interests** (our justifiable business aims) but only if those interests are not outweighed by your other rights and freedoms (e.g. your right to privacy);
- Do something for which you have given your **consent**;
- Fulfil our **contractual obligations** to you; and
- Fulfil our **legal obligation**.

We do not generally rely on the **vital interests** or **public task** lawful bases (Article 6(1)(d) and 6(1)(e) GDPR). If this changes, we will update this Privacy Policy. We do not intentionally process **special category data** (Article 9 GDPR) or **criminal offence data** (Article 10 GDPR) unless this is necessary for a specific purpose and permitted by law, in which case we will provide the required additional information. This does not prevent you from choosing to provide information that could be considered special category data in free-text fields (for example, in support communications); where such information is provided, we will process it only as necessary to respond and provide the services and in accordance with applicable law. Where our customers upload special category or criminal offence data into Kube as part of their use of the service, they remain controller and are responsible for identifying an Article 9 or 10 condition; the terms governing our processing of that data are set out in the Data Processing Addendum.

7.2 The section below explains the legal reasons (lawful bases) we rely on when we use your personal data. If we start using your personal data for a new purpose, we will update this Privacy Policy.

7.2.1 **Legitimate interests**: we may use your personal data where this is necessary for our legitimate interests (our business purposes), provided those interests are not overridden by your rights and freedoms.

For example, we may rely on legitimate interests to:

- improve and optimise our Website/Site;
- monitor and improve our Website/Site to enhance security and prevent fraud;
- provide our services to you and ensure the proper functioning of our Website/Site;
- provide services, features and benefits to members of our community; and
- protect our business and defend legal claims.

When we rely on legitimate interests, we consider whether our use of personal data is necessary for that purpose and whether it is overridden by your rights and freedoms.

7.2.2 Consent

We may rely on consent where you have asked us to use or share your personal data in a particular way, or where you have agreed to receive marketing from us. You can withdraw your consent at any time.

7.2.3 **Contract**

This is in order to perform our obligations to you under a contract we have entered into with you.

7.2.4 Legal Obligation

We may rely on this lawful basis where we need to use your personal data to comply with a legal obligation.

7.3 Where we need to collect your personal data (for example, in order to fulfil a contract, we have with you), failure to provide us with your personal data may mean that we are not able to provide you with the services. Where we do not have the information required about you to fulfil a service, we may have to cancel the service ordered.

7.4 The table below explains the main purposes for which we use your personal data and the lawful basis we rely on.

7.4.1 Where we rely on legitimate interests, we explain what those interests are.

7.4.2 Some purposes may have more than one lawful basis depending on the circumstances. If you would like more information about the lawful basis we rely on in a particular case, please contact us using the details at the start of this Privacy Policy.

Purpose	Legal Reason(s) for using the personal information
To enrol you as a customer	Contract Reason, Legitimate Interests Reason (in order to offer you other goods, services and/or digital content which helps us to develop our business)
To enrol you as a member of our community	Legitimate Interests Reason (to enrol and manage community membership, enable participation in community activities, and provide community related services and benefits to members)
To process your order, which includes taking payment from you, advising you of any updates in relation to your order or any enforcement action against you to recover payment	Contract Reason, Legitimate Interests Reason (in order to recover money that you owe us)
To manage our contract with you and to notify you of any changes	Contract Reason, Legal Obligation Reason
To comply with audit and accounting matters	Legal Obligation Reason
For record keeping, including in relation to any guarantees or warranties provided as part of the sale of goods, services, and/or digital content	Contract Reason, Legal Obligation Reason
To improve the goods, services, and/or digital content that we supply	Legitimate Interests Reason (in order to improve the goods, services, and/or digital content for future customers and to grow our business)
To recommend and send communications to you about goods, services, and/or digital content that you may be interested in.	Legitimate Interests Reason (in order to grow our business), Consent Reason
To ensure the smooth running and correct operation of our website	Legitimate Interests Reason (to ensure our website runs correctly)
To understand how customers and visitors to our website use the website and interact with it via data analysis	Legitimate Interests Reason (to improve and grow our business, including our website, and to understand our customer's needs, desires, and requirements)

8. Who we share your information with

8.1 We share (or may share) your personal data with:

- Our personnel: our employees (or other types of workers) who have contracts containing confidentiality and data protection obligations.
- Service providers (sub-processors) who help us operate our business and provide our Website/Site and services, such as cloud hosting and infrastructure providers;
- customer support and ticketing providers;
- analytics and security monitoring providers;
- professional advisers (including legal, insurance and accounting); and
- marketing and outreach providers (including Prospect Global Ltd (trading as Sopro), where applicable).

We ensure these organisations only have access to the information required to provide the services and that we have appropriate contractual protections in place.
A current list of our sub-processors is published at kuberno.com/sub-processors. We will notify our customers in accordance with the Data Processing Addendum before appointing a new sub-processor.

8.2 If we were asked to provide personal data in response to a court order or legal request (e.g. from the police), we would seek legal advice before disclosing any information and carefully consider the impact on your rights when providing a response.

8.3 We do not sell your personal information for money. We also do not share your personal information for cross-context behavioral advertising as those terms are defined under applicable US privacy laws (including the California Privacy Rights Act), except where you direct us to do so or where permitted by law and subject to any applicable right to opt out.

9. Where your information is located or transferred to

9.1 We store your personal data primarily in the UK and the EEA.

9.2 Where we transfer personal data outside the UK/EEA, we will do so using an appropriate safeguard, such as (as applicable) an adequacy decision, the EU Standard Contractual Clauses (SCCs), the EU-US Data Privacy Framework and the UK Extension to the Data Privacy Framework (for transfers to certified recipients in the United States), and/or the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs. Depending on the services used, transfers may be made to destinations such as the United States and other jurisdictions in which our sub-processors operate. A current list of our sub-processors, the destination countries and the safeguards in place for each is available at kuberno.com/sub-processors.

9.3 You may request further information about international transfers and obtain a copy of the relevant safeguards by contacting us using the privacy contact details in this Privacy Policy.

10. Automated decision making

10.1 'Automated decision making' is where a decision is automatically made without any human involvement. Under data protection laws, this includes profiling. 'Profiling' is the automated processing of personal data to evaluate or analyse certain personal aspects of a person (such as their behaviour, characteristics, interests, and preferences).

10.2 Data protection laws place restrictions upon us if we carry out any automated decision making (including profiling) that produces a legal effect or similarly significant effect on you. We may carry out limited profiling (for example, basic analytics or segmentation) that does not have such effects.

10.3 We do not make decisions about you that are based solely on automated processing (including profiling) where the decision produces a legal effect or a similarly significant effect on you (Article 22 GDPR). If this changes, we will update this Privacy Policy.

11. How we keep your information safe

11.1 These measures include:

- Access controls and user authentication (including multi-factor authentication);
- Internal IT and network security;
- Regular testing and review of our security measures;
- Staff policies and training;
- Incident and breach reporting processes;
- Business continuity and disaster recovery processes; and
- Maintaining recognised information security standards. We operate our information security management practices in line with recognised industry standards, including ISO/IEC 27001 and SOC 2 Type II, which are independently assessed frameworks designed to help ensure the confidentiality, integrity, and availability of information. We publish information about our information security certifications, including ISO/IEC 27001 and SOC 2, on our website.

11.2 If there is an incident affecting your personal data and we are the controller, we will notify the relevant regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach (where required by law). Where the breach is likely to result in a high risk to individuals, we will also inform affected individuals without undue delay (where required by law).

11.3 Where we act as a processor for the affected personal data, we will notify the relevant controller without undue delay and in any event within the timeframe specified in the applicable Data Processing Addendum, and support the controller with investigating and responding to the incident.

11.4 If you notice any unusual activity on the Website/Site, please contact us using the details in the Contact Details section above.

12. How long we keep your information

12.1 Where we act as the controller, we will only retain your personal data for as long as necessary to fulfil the purposes we collected it for. Please see retention periods table in Section 4.

12.2 To decide how long to keep personal data (also known as its retention period), we consider the volume, nature, sensitivity of the personal data, the potential risk of harm to you if an incident were to happen, whether we require the personal data to achieve the purposes we have identified or whether we can achieve those purposes through other means (e.g. by using aggregated data instead), and any applicable legal requirements (e.g. minimum accounting records for HM Revenue & Customs).

12.3 In some cases, we may need to keep certain records for longer than the indicative periods in the table (for example, where we need to comply with legal obligations or defend legal claims). For example, we may keep Identity Data, Contact Data, and certain communications for up to seven years after the end of our contractual relationship with you where necessary for compliance, accounting or legal purposes.

12.4 If you browse our Website, we keep personal data collected through analytics tools only for as long as necessary for the purposes described in this Privacy Policy. If you have asked for information from us or subscribed to our mailing list, we keep your details until you ask us to stop contacting you (subject to any legal requirements to retain suppression lists to respect your preferences).

13. Children's data

Our Website/Site and services are not intended for children, and we do not knowingly collect personal data from children. If you believe a child has provided us with personal data, please contact us and we will take steps to delete the information where appropriate.

14. Our role as controller and processor

For our Website, marketing, sales, customer support metadata, billing and business-contact relationships, we act as a controller. When our customers upload, create or otherwise process personal data through Kube as part of using the service, we act as a processor on behalf of that customer, who is the controller; the detailed terms of our processing are set out in the Data Processing Addendum to each customer agreement. Where we act as a processor, our customers are responsible for providing relevant notices to individuals and for handling rights requests, and we support them as required.

15. Your legal rights

15.1 You have specific legal rights in relation to your personal data.

15.2 We may need to confirm your identity before we can respond to a request (this is one of our security processes to make sure we keep information safe). We will only request information that is reasonably necessary to verify your identity, for example by confirming you control an account-linked email address or asking for additional information where proportionate. We can decide not to take action where we have

been unable to confirm your identity, or if we consider the request manifestly unfounded or excessive (in which case we may instead charge a reasonable fee). If this happens, we will inform you in writing.

15.3 We will respond to your legal rights request without undue delay, but within one month of us receiving your request or confirming your identity (whichever is later). We may extend this deadline by two months if your request is complex, or we have received multiple requests at once. If we need to extend the deadline, we will let you know and explain why we need the extension.

15.4 We do not respond directly to requests which relate to personal data for which we act as the processor. In this situation, we forward your request to the relevant controller and await their instruction before we take any action.

15.5 If you wish to exercise any of the rights listed below, you can reach us at privacy@kuberno.com.

Access:

You can ask for a copy of your personal data and information about how we use it.

Rectification:

You can ask us to correct personal data if it is inaccurate or incomplete.

Erasure:

You can ask us to delete your personal data where you are entitled to do so.

Restriction:

You can ask us to restrict how we use your personal data in certain circumstances.

Object:

You can object to our use of your personal data in certain circumstances, including where we use it for direct marketing.

Withdraw consent:

Where we rely on your consent, you can withdraw it at any time. This will not affect the lawfulness of processing before you withdrew consent.

Portability:

You can ask us to send you or another organisation an electronic copy of your personal data.

Automated decision-making:

You have the right not to be subject to certain decisions based solely on automated processing, including profiling, where it produces legal or similarly significant effects on you.

Complaints:

If you are unhappy with the way we collect and use your personal data, you can complain to the ICO (in the UK) or another relevant supervisory authority (for example, in the EEA). We would, however, appreciate the chance to deal with your concerns first, so please contact us at privacy@kuberno.com.

16. When we send you marketing messages

16.1 We market to prospective and existing business customers; this is known as Business-to-Business Marketing (B2B Marketing). We may send marketing communications using work contact details. For data protection purposes, where permitted by law we may rely on our legitimate interests to send B2B marketing. However, the rules on electronic marketing (including email) may require consent or may only permit marketing in limited circumstances (for example, where the "soft opt-in" applies). Where consent is required, we will obtain it and you can withdraw it at any time. We may also contact you by telephone where permitted and may screen numbers against relevant preference services where required. You can opt out at any time by using the unsubscribe/opt out link in the message or by contacting us at privacy@kuberno.com.

16.2 Opting out of marketing will not affect our processing of your personal data in relation to any order you have with us or where we are required to use your personal data to fulfil that order or provide you with certain information.

16.3 We may appoint digital marketing agents to support our marketing activity. Where we use third-party prospecting providers (including Prospect Global Ltd (trading as Sopro) Reg. UK Co. 09648733), they may provide us with business contact details sourced from permitted sources. We require such providers to act under contract and to support us with complying with applicable data protection and direct marketing laws, including maintaining suppression lists and honouring opt-outs.

17. Third-party websites

Our website may contain links to third-party websites. If you click and follow those links, then these will take you to the third-party website. Those third-party websites may collect personal information from you, and you will need to check their privacy notices to understand how your personal information is collected and used by them.

18. Additional information for US and California residents

If you are a resident of the United States, including California, you may have additional rights in relation to your personal information under applicable US privacy laws. These laws may include the California Consumer Privacy Act (as amended by the California Privacy Rights Act), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Texas Data Privacy and Security Act, the Oregon Consumer Privacy Act, the Montana Consumer Data Privacy Act, the Tennessee Information Protection Act, the Florida Digital Bill of Rights, the Delaware

Personal Data Privacy Act, and other comparable state laws as they come into force. Depending on your state of residence, you may have the right to access, delete or correct your personal information, to opt out of certain processing (including targeted advertising and the sale or sharing of personal information), to limit the use and disclosure of sensitive personal information, to appeal a refusal to action your request, and to designate an authorised agent to act on your behalf. We will respond to verifiable requests within the time periods required by the applicable state law (typically 45 days, extendable by a further 45 days where reasonably necessary). Where required by applicable law, we will provide additional state-specific disclosures (including the categories of personal information we collect and disclose, the purposes for which we use it, the categories of sources and recipients, whether we process sensitive personal information, our retention periods (or criteria used to determine them), and whether personal information is used for targeted advertising) in a clear and accessible notice made available at or before the point of collection (including through this Privacy Notice and/or a supplemental notice), and we will not require you to submit a separate request solely to access those disclosures.

Retention: We retain personal information for as long as reasonably necessary for the purposes described in this Privacy Notice, including to provide the services, maintain business records, comply with legal obligations, resolve disputes, and enforce our agreements. Retention periods vary by category of personal information and are determined based on the nature of the data, the purposes for which it is processed, and applicable legal requirements.

Targeted advertising; sale/sharing: We do not sell personal information for money. We may use limited online identifiers and usage information to measure and deliver advertising, including interest-based advertising, where permitted by law. To the extent our advertising activities constitute “sharing” for cross-context behavioural advertising under applicable law, you may have the right to opt out of such sharing (and any sale or sharing of personal information as those terms are defined under applicable law).

Sensitive personal information: Depending on how you use the services, we may collect and process limited sensitive personal information (for example, account log-in credentials and, where you choose to provide it, information that may reveal health or other sensitive characteristics in support communications). For clarity, “sensitive personal information” as used here may include information treated as “special category data” under the GDPR if you choose to provide it in free-text fields; we do not request such information and do not use it to infer characteristics about you. We use sensitive personal information only as reasonably necessary to provide the services, secure our systems, prevent fraud, and comply with law.

Categories of personal information we collect and disclose: We collect and may disclose (to service providers/processors and, where applicable, other recipients described in this Privacy Notice) identifiers and contact details; account credentials; customer and support communications; payment and transaction information; device, browser, and network information; usage and analytics data; and other information you choose to provide. We do not knowingly collect personal information from children.

For convenience, the information below summarises key disclosures that may be required under certain US state privacy laws. This summary is provided at a high level and may be supplemented by a point-of-collection notice or other state-specific disclosures where required.

Appeals (certain US states): If we decline to take action on your request, you may appeal our decision by replying to our response or contacting us using the privacy contact details in this Privacy Policy with the subject line “Privacy Rights Appeal”. Please include the state you reside in and the request you are appealing. We will respond to your appeal within the time period required by applicable law. If your appeal is denied, we will provide information on any further steps available to you under applicable law (which may include contacting your state Attorney General or other regulator).

For the avoidance of doubt, we do not sell personal information for money. We may disclose personal information to service providers and other processors that perform services on our behalf (for example, hosting, analytics, customer support, security, and payment processing), and to professional advisers and authorities where required by law.

California residents may have the right to:

- request access to personal information;
- request deletion;
- request correction;
- opt out of the sale or sharing of personal information (as those terms are defined under California law); and
- limit the use and disclosure of sensitive personal information (where applicable).

You may exercise these rights by (i) using the “Do Not Sell or Share My Personal Information” link (or equivalent setting) available in the product or on our website, (ii) enabling an opt-out preference signal such as Global Privacy Control (GPC) where supported, or (iii) contacting us using the privacy contact details in this Privacy Policy.

We do not discriminate against you for exercising your privacy rights. Where required by law, we will recognise opt-out preference signals such as Global Privacy Control (GPC) for the browser or device you use, in a way that is straightforward for you to use.