

Helm Compliance – Privacy Policy

Regulatory Compliance SaaS (HelmHub) Last updated: February 2026

1. Introduction

Helm Compliance (“we”, “us”, “our”) operates the HelmHub regulatory compliance software-as-a-service platform. We are committed to protecting your privacy and handling your personal data in accordance with applicable data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and, where relevant, the EU General Data Protection Regulation (EU GDPR) and other global privacy standards. This Privacy Policy explains what personal data we collect, how we use it, who we share it with, how long we keep it, and what rights you have. It applies to: - Visitors to our website and marketing pages - Individuals who register for, access, or use the HelmHub Service - Representatives of organisations that subscribe to the Service (e.g. account administrators, billing contacts) - Any other individuals whose personal data we process in connection with the Service By using our website or the Service, you acknowledge that you have read and understood this Privacy Policy. If you do not agree, please do not use our website or the Service.

2. Who We Are and How to Contact Us

Data controller: Helm Compliance (or the legal entity identified in your order or on our website) is the data controller for the personal data we process in connection with our website and the HelmHub Service. Contact: - Email: support@helmcompliance.com - Website: www.helmcompliance.com - Address: As published on our website For data protection enquiries or to exercise your rights, you may contact us using the details above. You also have the right to lodge a complaint with a supervisory authority (e.g. in the UK, the Information Commissioner's Office – ico.org.uk).

3. What Personal Data We Collect and Why

We collect and use personal data only where we have a lawful basis (e.g. contract, consent, legitimate interest, or legal obligation). The following describes the main categories of data and purposes. 3.1 Account and Service Use - Name, email address, and contact details – To create and manage your account, authenticate you, and communicate about the Service (e.g. login, password reset, support, billing). - Organisation name and details – To set up and administer your organisation's subscription and to provide the Service. - Role and permissions – To enforce access control (e.g. Organisation Admin, Compliance Manager, Auditor, Consultant) and to provide the correct features and data access. - Usage and activity data – To operate the Service, provide support, improve the product, and ensure security (e.g. audit logs of actions, IP address, user agent). Lawful basis: Performance of our contract with you or your organisation; legitimate interests (security, improvement, support); and, where required, consent or legal obligation. 3.2 Billing and Payment - Billing contact name, email, and address – To send invoices, manage subscriptions, and communicate about payment. - Payment-related data – Payment processing is handled by our payment provider (e.g. Stripe). We do not store full card numbers; we may store or receive references necessary for billing (e.g. last four digits, billing history). Cardholder data is processed in accordance with our payment provider's terms and applicable standards (e.g. PCI DSS where applicable). Lawful basis: Performance of contract; legal obligation (e.g. tax, accounting). 3.3 Marketing and Communications - Email and preferences – If you have opted in or we have a legitimate interest (e.g. existing customer communications), we may send you product updates, security notices, or marketing. You can opt out of marketing at any time. - Website and marketing site – We may collect technical and usage data (e.g. IP address, browser type, pages visited) to operate and improve our website and to analyse usage. Where we use cookies or similar technologies, we will do so in line with applicable law and our cookie notice. Lawful basis: Consent (where required for marketing); legitimate interest (website operation, analytics); legal obligation where applicable. 3.4 Data You Put Into the Service (Customer Data) When you or your organisation use the Service, you may upload or create data that contains personal data (e.g. names, contact details of staff or consultants in procedures, evidence, or reports). We process this data only as a processor on your behalf to provide the Service, in accordance with our Terms of Service and any data processing agreement. You (or your organisation) remain the data controller for that data; we do not use it for our own purposes (e.g. marketing or product development) except as necessary to operate and support

the Service, or as required by law.

4. How We Use Your Personal Data

We use personal data to: - Provide, operate, and support the HelmHub Service - Create and manage accounts, authenticate users, and enforce access control - Process payments and manage subscriptions - Communicate with you about the Service (e.g. support, security, product updates) - Send marketing only where you have consented or where we have a lawful basis - Comply with legal and regulatory obligations (e.g. tax, audit, law enforcement) - Protect the security and integrity of the Service and our systems (e.g. audit logs, incident response) - Improve our products and services (e.g. analytics, in an aggregated or anonymised form where appropriate) We do not sell your personal data to third parties.

5. Who We Share Your Personal Data With

We may share personal data with: - Sub-processors and service providers – To operate the Service (e.g. cloud hosting such as AWS, payment processing such as Stripe, email delivery, and where applicable AI or other tools). We ensure appropriate contracts and safeguards (e.g. data processing terms, confidentiality) are in place. - Professional advisers – Where necessary (e.g. lawyers, auditors) under confidentiality. - Regulators and authorities – Where required by law (e.g. supervisory authorities, law enforcement). - Other parties – Only with your consent or where required or permitted by law. We do not share your personal data with third parties for their marketing purposes.

6. International Transfers

The Service is hosted in the United Kingdom and/or other locations (including via Amazon Web Services). If you or your users access the Service from outside the UK/EEA, your data may be transferred to and processed in the UK or other countries where we or our service providers operate. We ensure appropriate safeguards where required by law, including: - Transfers to countries recognised as providing an adequate level of data protection (e.g. UK adequacy decisions) - Standard contractual clauses (UK and/or EU) or other approved mechanisms where adequacy does not apply Details of sub-processors and transfer mechanisms can be provided on request.

7. How Long We Keep Your Personal Data

We retain personal data only for as long as necessary to: - Fulfil the purposes set out in this Privacy Policy - Comply with our legal, tax, and regulatory obligations - Resolve disputes and enforce our agreements Retention periods depend on the type of data and purpose (e.g. account data for the duration of the subscription and a limited period after termination; audit logs in line with our retention policy; billing data as required for tax and accounting). After the retention period, we delete or anonymise the data in accordance with our procedures.

8. Your Rights (UK GDPR and Applicable Law)

Under the UK GDPR and applicable data protection law, you may have the right to: - Access – Request a copy of the personal data we hold about you - Rectification – Request correction of inaccurate or incomplete data - Erasure – Request deletion of your personal data in certain circumstances - Restriction – Request that we restrict processing in certain circumstances - Data portability – Request a copy of your data in a structured, machine-readable format where applicable - Object – Object to processing based on legitimate interests or for direct marketing - Withdraw consent – Where we rely on consent, you may withdraw it at any time - Lodge a complaint – With a supervisory authority (e.g. the ICO in the UK) To exercise any of these rights, please contact us using the details in section 2. We will respond within the time limits required by applicable law (e.g. one month under the UK GDPR, subject to extensions where permitted). We may need to verify your identity before processing your request. Some rights may be limited (e.g. where we must retain data for legal obligations or where we process data as a processor on behalf of your organisation). Where we act as processor, we will assist the data controller (e.g. your organisation) in responding to your rights.

9. Security

We implement appropriate technical and organisational measures to protect your personal data against unauthorised access, loss, alteration, or disclosure, in line with our Security Policy and applicable law. This includes access control, encryption in transit, secure storage, audit logging, and incident response procedures. For more detail, see our Security Policy.

10. Children

The Service is not intended for individuals under the age of 18 (or the age of majority in your jurisdiction). We do not knowingly collect personal data from children. If you believe we have collected data from a child, please contact us and we will take steps to delete it.

11. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, the Service, or the law. We will post the updated policy on our website and, where appropriate, notify you (e.g. by email or a notice in the Service). The "Last updated" date at the top indicates when the policy was last revised. We encourage you to review this policy periodically.

12. Additional Information for Certain Jurisdictions

- UK and EEA: This policy is written to comply with the UK GDPR and, where relevant, the EU GDPR. - Other jurisdictions: If you are located outside the UK/EEA, we will process your data in accordance with this policy and applicable local law. Where local law requires additional disclosures or rights, we will comply. For specific questions about how we handle your data in your jurisdiction, please contact us.

13. Contact

For any questions about this Privacy Policy or our handling of your personal data: - Email: support@helmcompliance.com - Website: www.helmcompliance.com - Address: As published on our website Document version: 1.0 | February 2026 | Helm Compliance

