Y.O.D.O. Ltd – Privacy Policy

Effective Date: 1 September 2025
Last Updated: 1 September 2025

This Privacy Policy explains how Y.O.D.O. Ltd ("Y.O.D.O.", "we", "us") collects, uses, stores, and protects your personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

---

1. Who We Are

Y.O.D.O. Ltd, registered in England and Wales under company number 15736034, is the data controller for purposes of UK data protection laws.

Governance
Data protection responsibilities are overseen directly by Y.O.D.O.'s leadership team. Currently, these responsibilities are carried out by the co-founder, who performs duties equivalent to a Data Protection Officer (DPO) until a statutory DPO is formally appointed. Y.O.D.O. regularly reviews its obligations under UK GDPR and will appoint a statutory DPO when legally required.

Contact: info@yodo.ltd
Address: 42 Mayfair Gardens, Southampton, SO15 2TW, United Kingdom

---

2. Data We Collect

We collect the following categories of personal data:

- **User data**: name, email, optional phone number, date of birth (recommended for verification).
- **Delegate data**: name, email, phone number (optional), identity verification data.
- **Special Delegate data**: name, profession, email, phone number (optional), verification details.
- **Recipient data**: name, email, and identity verification data (collected only at the time a message is triggered).
- **Identity documentation**: for verification purposes (via Persona or iDenfy).
- **Sealed message metadata** (never content).
- **Check-in logs** (active and passive).
- **Minimal biometric data** (optional and consent-based, e.g., heart rate for passive check-ins).
- **Technical data:** IP address, browser agent, device identifiers, and similar information collected automatically for security monitoring and analytics.

---

3. Why We Collect Data

We process personal data to:

- Deliver and operate the Y.O.D.O. platform.
- Verify User, Delegate, Special Delegate, and Recipient identity, and confirm passing events.
- Enable secure message delivery.
- Maintain accurate audit logs.
- Support Delegate and Special Delegate account functionality (notifications, verification duties).
- Comply with legal and contractual obligations.
- Detect and prevent fraudulent or unauthorized access, and monitor security of our services.

---

4. Lawful Basis for Processing

We process personal data under lawful bases including consent, contract, legitimate interests, and legal obligations, as outlined in the Appendix.

---

5. Sharing of Data

We may share personal data with trusted providers, including Cloudflare, Render (hosting), Crunchy Data (database), Persona/iDenfy, Twilio/Resend, AWS S3 (storage), Google Analytics/GTM, and Cookiebot. Each provider's independent terms and policies apply.

---

6. Data Retention

We only keep personal data for as long as necessary for the purposes described in this Policy.

Data Type	Retention Period	Notes
User & Delegate accounts	While account is active	Deleted upon closure, subject to regulatory logs
Special Delegate accounts	While active	Deleted upon withdrawal, with audit logs retained securely
Sealed messages	Until triggered + 30 days	Deleted permanently if undownloaded
Check-in data	Deleted after 60 days inactivity	Includes a 30-day grace + 30-day pre-deletion phase
Backups	30 days	Then securely purged

Data Type	Retention Period	Notes
Death certificates	Deleted immediately after verification	Never stored permanently

---

7. Your Rights

Under UK GDPR, you may request access, correction, deletion, restriction, objection, or portability of your data.
We may require proof of identity before fulfilling such requests.
Special Delegates and Recipients may also contact us directly to exercise their rights.

---

8. Security Measures

We implement strong technical and organizational safeguards including:

- Encryption (in transit & at rest)
- Role-based access controls and audit logs
- Administrator access protected by Cloudflare Zero Trust, requiring identity verification and device security checks.
- Staff privacy and security training
- Regular backups and secure deletion protocols
- Data breach response procedures

In the event of a personal data breach, we will notify affected individuals and relevant regulators **without undue delay**, and in any case **within 72 hours** where legally required under UK GDPR.

---

9. Cookies and Tracking

We use cookies and similar technologies for:

- **Essential functions** – account login, security, and platform operation.
- **Functional cookies** – remembering your settings and preferences.
- **Analytics** – understanding platform usage (via Google Analytics/GTM).
- **Verification and consent management** – managed via Cookiebot.
- **Marketing cookies (only if consented)** – to deliver tailored updates or offers.

Cookie retention varies but generally does not exceed 24 months. You can manage or withdraw consent at any time through our Cookie Notice or your browser settings.

---

10. Automated Decision-Making

We do not use automated decision-making or profiling with legal or significant effects.

---

11. Children's Data

We do not knowingly collect personal data from children under 18 without verified parental or guardian consent. Where a User has designated a Recipient who is under 18, access to any message will only be granted once parental or guardian consent and identity verification are completed. If verified consent is not provided, the message will not be delivered.

11A. International Data Transfers

We may transfer or store personal data outside the UK. Where we do so, we rely on:

- Adequacy regulations issued by the UK Government, or
- Standard Contractual Clauses (SCCs) approved by the UK Information Commissioner's Office (ICO).

These mechanisms ensure that your personal data continues to receive a level of protection essentially equivalent to UK GDPR standards.

---

12. Changes to This Policy

We may update this Privacy Policy; material changes will be communicated directly.

---

13. Contact

Email: info@yodo.ltd
Mail: Y.O.D.O. Ltd, 42 Mayfair Gardens, Southampton, SO15 2TW, United Kingdom
You may also contact the Information Commissioner's Office (ICO): https://ico.org.uk

---

Appendix: Lawful Basis Mapping

Processing Activity	**Data Collected**	**Lawful Basis (Art. 6)**	**Special Category Basis (Art. 9)**
Account creation & login	Name, email, password, DOB	Contractual necessity	–
Identity verification	ID scans, selfies, biometric data	Contractual necessity / Legitimate interest	**Art. 9(2)(a) – explicit consent**, or **Art. 9(2)(f) – legal claims/fraud prevention**
Delegate/Recipient management	Contact info	Contractual necessity /	–

Processing Activity	Data Collected	Lawful Basis (Art. 6)	Special Category Basis (Art. 9)
		Legitimate interest	
Check-ins (active/passive)	Logs, responses	Contractual necessity	–
Passive health check-ins	Heart rate/physiological signals	Consent	**Art. 9(2)(a) – explicit consent**
Message storage/delivery	Message metadata (sealed content)	Contractual necessity	–
Death verification	Death certificates (Delegates/Special Delegates)	Legitimate interest / Legal obligation	**Art. 9(2)(f) – legal claims**, or **Art. 9(2)(a) – explicit consent of provider**
Notifications & alerts	Delegate/Recipient contact info	Contractual necessity	–
Marketing communications	Email address	Consent	–
Payment processing	Payment data (via Stripe/PayPal)	Contractual necessity	–
Security monitoring	IP, access logs	Legitimate interest	–
Compliance/audit	Logs, certificates	Legal obligation	–