Privacy Notice

Effective date: 10 December 2026

Part A

1. Introduction

This Privacy Notice explains how The Messaging Company Pty Ltd (ACN 669 674 382), other entities in its corporate group, and its local agents and/or associates (together “we”, “our” or “us”) collect, use, store, share, and safeguard personal data in accordance with the data protection laws that apply to you. It also outlines the rights you have in relation to your personal data, including to access, rectify, or update the information we hold about you. The law and regulator that apply in your region are set out in Part B, and the corresponding regional terms are in Part C.

2. Our role

Our role differs depending on the type of personal data and how you come to use our services.

For the content that you create, send, receive, or store through the email service (including emails, contacts, calendar entries, tasks, and attachments) (together “Content”), we are not the data controller. We process that Content on your behalf to provide the services in accordance with our agreement with you.

For account and billing data (including the identifying, account, contact, and purchase and transaction information used to establish, administer, bill, and support the account), we act as the data controller.

Our staff do not routinely access, read or analyse the Content of your email. Other than for the automated processing described in section 5, we access it only where necessary to operate, maintain, secure and provide the service, or where the law requires.

3. Personal data we collect

In this Privacy Notice, we use the term “personal data”. When we use this term, we mean information that can identify or be linked to you as an individual.

We collect different types of personal data depending on how you interact with us. This includes information you provide directly, information collected automatically through your use of our services, and information obtained from third parties.

Information you provide directly

We collect personal data that you choose to provide to us, for example when you create an account, communicate with us, or purchase our products or services.

This may include:

- your full name and date of birth;
- account information, including your username;
- contact details such as your residential and billing addresses, phone number(s), and email address(es);
- purchase and transaction information, including details about payment methods and payments to and from you, and other details of services and products you have purchased from us;
- marketing preferences, including your choices about receiving marketing communications from us;
- records of our interactions and correspondence with you via phone (including call recordings and automatic transcripts), when submitting a web form or online chat interaction, email, text message, social media, or otherwise;
- customer service information, including your customer service enquiries and comments, feedback, and survey responses;
- information required to meet our legal obligations (including data relating to contracts, payments, and communications sent or received via our services); and
- a copy of any email reported as misclassified (e.g. spam, not spam, phishing, malware, etc.).

Information collected automatically

When you use our websites, mobile applications, or online services, we automatically collect certain information about your device and activity.

This may include:

- usage data about how you interact with our services;
- IP address and general location information derived from your IP address (not precise location);
- search and browsing behaviour and user journeys;
- website usage patterns;
- cookie preferences;

- information collected from cookies, beacons, tags, and scripts, including details about your interaction with our online presences, such as the pages you visit, the number of visits, the number of scrolls, language preferences, webpage interactions and searches, IP address, and the location of the devices accessing our websites and services, demographic information about you, your user settings, and analytics data; and

- log file information automatically reported by your internet browser or mobile application each time you access our websites or services, including information such as your operating system, device type, unique identification number, browser type, geographic location, referring/exit pages and URLs, number of clicks, domain names, landing pages, and pages viewed.

Information obtained from third parties or linked accounts

We may also receive information about you from third parties, including when you link or integrate third-party services with your account.

This may include:

- information about any third-party accounts you connect or link to your account with us;

- technical information or metadata received through linked accounts or services (e.g. to retrieve or send emails, or to attach/save files); and

- verification or anti-fraud data obtained from payment processors or compliance partners where required by law.

The above list is not exhaustive and in specific instances we may need to collect additional personal data for the purposes set out in this Privacy Notice.

If you do not provide the personal data we require to deliver our products or services, we may be unable to provide certain features or services to you.

4. How we use your personal data

The table below explains the purposes for which we use your personal data and the corresponding legal basis.

Purpose	Legal basis
To operate, maintain, and provide to you (or your service providers) the features and functionality of our websites, products, and services	Performance of a contract
To process, manage, and deliver customer accounts	Performance of a contract
To provide you with quotations, updates, and information related to our services (including steps taken prior to entering into a contract)	Performance of a contract
To notify you about changes to our services, terms of service, or this Privacy Notice	Performance of a contract
To establish your identity and verify your account	Performance of a contract
To send you marketing communications (including newsletters or promotional materials)	Legitimate interests, including consent where the law requires it;

	you can opt out, or withdraw consent, at any time
To respond to your questions and concerns or to enable you to exercise your legal rights (such as data subject access requests)	Legal obligation
To comply with our legal obligations and other regulatory or compliance requirements	Legal obligation
To administer and protect our organisation, products, services, and websites, including troubleshooting, data analysis, testing, system maintenance, support, reporting, hosting, security, vulnerability and fraud detection, and protection activities	Legitimate interest - to ensure the effective and secure operation of our business and IT systems
To improve our websites, products, services, marketing, customer relationships, and user experiences (including through analytics and business intelligence)	Legitimate interest - to understand how our products and services are used and improve them
To aggregate or de-identify data for analysis and produce insights about the use of our services and websites	Legitimate interest - to develop and enhance our offerings
To research, monitor, and evaluate our products and services in order to improve quality and develop new offerings	Legitimate interest - to innovate and enhance our service delivery
To monitor or audit your use of our products, services, and equipment for compliance with contractual terms or applicable law	Legitimate interest - to ensure your compliance and protect our rights
To minimise the risk of or prevent fraud, crime, or misconduct	Legitimate interest - to protect our business, users, and partners
To enhance or ensure the safety and security of our and others' employees, customers, suppliers, and systems	Legitimate interest - to maintain a safe and secure environment
To help our partners (or other customers to whom we provide services on their behalf), such as antiabuse partners, to improve their services or online offerings	Legitimate interest - to support our partners' improvement and innovation activities
To send you educational information (e.g. scam education and new product features) related to the email service we provide to you	Legitimate interest - to help you learn how to use and protect your email account

Identity verification

When you sign up, we use your name, date of birth, phone number, and email address to establish your identity, confirm you are at least 18 years of age, and set up your account. We do this to perform our contract with you and to protect your account against impersonation.

We verify your email address and mobile phone number through a confirmation step; the other details you give us are self-declared and not independently checked.

Use of artificial intelligence (AI)

Our suppliers, acting on our behalf, may process personal data using AI within controlled environments. One example is an AI assistant that helps us handle support requests, but we may also use AI to develop and improve other parts of our products and services, such as security, spam and abuse detection, reliability, service quality, and customer experience.

We do not use your personal data to train publicly available or general-purpose third-party AI models. What you enter into these tools, and the resulting interactions, may be used to improve our own AI

models. Any development or improvement of our own models is carried out by our suppliers on our behalf, on our own data (which may include personal data) and in controlled environments. We use de-identified or anonymised data for this purpose wherever possible. The personal data used for this purpose is limited to what is necessary and we apply data-minimisation and confidentiality safeguards to it.

Automated decision-making

We may use artificial intelligence and/or automated processing tools to help deliver our services and protect our customers. Some of these programs can make, or help us make, decisions about your account and messages.

Decisions made solely by a computer program may include:

- Suspension or cancellation: If a payment is overdue, our billing system may automatically suspend and/or cancel your account, according to timeframes listed in our Terms of Service.

- Reactivation: Access may be restored automatically on receipt of payment. If the account remains unpaid, the account and its data are automatically deleted in accordance with timeframes listed in our Terms of Service.

- Service restriction: If your account exceeds its storage allowance, our systems may automatically restrict the sending and receiving of emails until storage is reduced or your plan is upgraded. You can still access your account.

- Compromised account: If your account appears to be compromised, we may automatically end sessions, block sending, remove forwarding rules, and reset your password.

- Login attempts: We may automatically refuse suspicious login attempts and/or temporarily lock your account after repeated use of incorrect passwords. We typically automatically unblock accounts in 24 hours.

- Outgoing email: We may pause sending if you exceed your sending limits. We may also refuse or downgrade delivery of messages flagged as spam, phishing or malware.

- Incoming emails: We may refuse, delay, quarantine, junk or delete messages based on the sender's reputation, location or authentication, or on spam, phishing and malware checks. Some high-risk messages are removed without notice to you or the sender.

- Account status: Accounts that haven’t opted in to a required transfer, or that are in a billing or sign-up status, may be restricted until the issue is resolved. Temporary access may be granted, and gets shorter each time it’s requested.

- Data deletion: Spam and Trash are emptied automatically after set periods. Deleted accounts are permanently removed after a grace period, and calendars and contacts are removed straight away. Some email addresses may be released for reuse after a hold period.

Decisions where computer programs substantially assist our staff:

- Abuse and security alerts: Where our system flags possible fraud, abuse, attacks, or breaches of our acceptable use policy and our staff decide whether to restrict an account or block a network.

- Support requests: Where our systems flag support requests that may be abusive, and our staff decide what action to take.

Personal data we use:

- Payment decisions: your billing and payment status, due dates and plan limits.
- Account security decisions: your IP address, login attempts, session information and email forwarding rules.
- Incoming and outgoing email decisions: the sender, the sending server, authentication results, your sending activity, and the content of messages and attachments, which can include sensitive information.
- Abuse and security alerts: your sending activity and the account and network activity linked to suspected fraud, abuse or attacks.

Where a decision is made by automated means that could affect your account, we apply the safeguards required by law, including meaningful human review and a way for you to contest the outcome. If you think an automated decision is incorrect, contact us at privacy@themessaging.co and a member of our team will review. See Part C for the rights that apply to your region.

6. Sharing and disclosure of personal data

We may share your personal data with the following categories of recipients, including to:

a) members of our corporate group, which means our subsidiaries, our ultimate holding company and its subsidiaries, and specifically Atmail Pty Ltd as a data processor;

b) our suppliers, service providers, agents, contractors, and partners who assist us with our business processes and the provision of our products and services, including Atmail Pty Ltd, which acts as one of our data processors and processes certain personal data on our behalf in connection with the hosting, operation, maintenance, and support of our email services, including in relation to:

i. helpdesk or chat services, namely Zendesk Inc, TTEC Holdings Inc, and Remote Technology Inc;

ii. information technology services, namely Microsoft Corporation, Cloudflare Inc, and Atlassian Pty Ltd;

iii. data processing, transfer, or hosting services, namely Amazon Web Services (AWS), Twilio Inc., and Stitch Data (Talend);

iv. third-party products and service providers whose products and services you purchase from us;

v. providing, managing, supporting, and improving our websites, products, services and organisation;

vi. Identity and authentication services, namely FusionAuth (Inversoft LLC), and fraud or other crime protection, credit reporting, or management services;

vii. business analysis and business intelligence services;

viii. customer relationship management system services, namely Zendesk Inc;

ix. payment processing services, namely Chargebee Inc, Stripe LLC, and PayPal Australia Pty Ltd;

x. anti-abuse services (e.g. antispam, antivirus, antimalware, and image classifiers, etc.), namely Abusix Inc, Data443 Inc, and Proofpoint Inc; and

xi. email delivery, marketing automation, and customer communication services, namely Maropost Australia Pty Ltd;

c) other persons authorised by you or who are responsible for or to you (such as guardians, persons holding power of attorney, lawyers, or executors);

d) regulators, law enforcement, national security agencies, or courts;

e) credit and debt collection services;

f) our professional advisers, including consultants, lawyers, bankers, auditors, audit assessors, insurers, risk assessors, or accountants who provide consultancy, legal, banking, auditing, insurance, risk management, or accounting services;

g) financiers, investors or third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets or that we acquire businesses or merge with (if a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Notice and also to evaluate our business and whether to proceed with a transaction with us); and

h) to third parties as required to protect the security or integrity of our services or to exercise or protect the rights, property, or personal safety of our company, our users, you, or others.

Any personal data you make publicly available on our websites or our service may be available to others to view. If you remove personal data that you have made public on our websites or on our service, copies may remain viewable in cached and archived pages of our websites or our service, or by other users who may have copied or saved that personal data.

7. International personal data transfers

Your personal data may be transferred to, and processed in, countries other than the one where you live, including:

- Australia
- Canada
- EEA (currently Ireland, Italy, Germany)
- United States
- Philippines
- India
- Singapore

Some of these countries may not offer the same level of data protection as your home country. Where such transfers occur, we ensure that they are carried out in compliance with applicable data protection laws. This includes implementing appropriate safeguards, such as transfers to countries

covered by an adequacy decision, or the use of standard contractual clauses that require the recipient to protect your personal data to an equivalent standard.

The safeguard depends on the destination:

- EEA locations and Canada - covered by adequacy and are not restricted transfers;
- Australia, Singapore, the Philippines, and India - rely on standard contractual clauses; and
- United States - relies on the relevant Data Privacy Framework where the recipient is certified, and otherwise on standard contractual clauses.

We complete a transfer risk assessment for the destinations that rely on safeguards. The specific transfer mechanism that applies to you, named under the law of your region, is set out in Part B and the corresponding regional terms in Part C.

We may transfer personal data to our affiliates, subsidiaries, and trusted service providers in these countries to support the operation of our services. Where we transfer personal data outside of the EEA, UK, or other regions with equivalent protection, we will ensure appropriate safeguards are in place in accordance with applicable data protection laws. This may include reliance on adequacy decisions, standard contractual clauses, or other legally recognised transfer mechanisms. Regardless of where your personal data is processed, we will take appropriate steps to ensure that it remains protected in accordance with this Privacy Notice and applicable data protection laws.

8. Personal data retention

We will retain your personal data while it is required for our business functions, or as is necessary to comply with our legal obligations, or to resolve disputes and/or enforce our agreements or rights under applicable laws. When we no longer need to retain your personal data for the purposes outlined above or as required by applicable law, our process is to destroy or de-identify the information.

When the service ends:

- **Personal data:** We retain your associated personal data for up to one hundred and twenty (120) days, and then delete or anonymise it, unless we are required by law to retain it for longer.
- **Account data:** We retain your account data for the life of your subscription and only for as long as necessary afterwards to meet our legal, regulatory, operational, and contractual obligations. Billing and payment records are retained for the period required by applicable tax and accounting laws; support requests for a reasonable period after they are resolved; security logs for a limited period; and marketing preferences are retained until your account is closed.

9. Your rights

Accuracy. It is important that the personal data you have provided to us is up-to-date, accurate and complete. Please keep us informed if your personal data changes during your relationship with us. If your details change you can update them by logging into your account to update your password, billing information, and other personal data.

Anonymous interaction. You have the option to engage with us anonymously. However, if you choose to interact with us anonymously, we may not be able to provide our products or services to you or make some offers available to you without your personal data.

Exercising your rights. Where you live determines your rights in relation to personal data. These may include the right to access a copy of the personal data we hold about you, to have inaccurate or incomplete data corrected, to have your data deleted where there is no lawful basis to continue processing it, to restrict processing in certain circumstances, to receive your data in a portable format, to object to processing based on our legitimate interests, and to withdraw consent where processing is based on consent. The specific rights that apply to you, and the law that grants them, are set out in the regional terms in Part C. To exercise any of these rights, please contact our Data Protection Officer using the details provided in this Privacy Notice.

Verification of identity and response times. We may need to request specific information from you to confirm your identity and to ensure your right to access your personal data (or exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to anyone who has no right to receive it. We aim to respond to all legitimate requests within one month. If your request is particularly complex or you have made multiple requests, we may take longer. In such cases, we will notify you and keep you informed of progress. We do not charge a fee for responding to your request unless we believe it is clearly unfounded, repetitive, or excessive, in which case we may charge a reasonable fee or refuse to act on the request.

Right to complain. You have the right to lodge a complaint with your local data protection supervisory authority if you believe that your rights have not been properly respected.

Automated decisions: You have the right to ask us to review a decision made by, or with the substantial help of, a computer program.

10. Security of your personal data

We implement appropriate technical and organisational measures, including industry-standard security controls, designed to protect personal data from loss, theft, misuse, and unauthorised access, disclosure, alteration, and destruction, taking into account the nature of the personal data that we process and the risks associated with that processing. Examples include:

- **Encryption:** Data in transit within our platform is protected using TLS 1.2 or higher, and data at rest is encrypted using AES-256. Encryption keys are held and controlled by Atmail Pty Ltd, our hosting provider. For email sent to external mail servers, we use the highest level of encryption the receiving server supports. If that server does not support TLS, the email may be sent without transport encryption. For incoming email, the sending server determines the encryption used. We cannot control the encryption standards used by systems outside our platform.

- **Access control:** System access is restricted by role-based permissions and enforced through multifactor authentication (MFA). Access is granted on the principle of least privilege.

- **Network security:** Firewalls, intrusion detection/prevention systems, and antimalware solutions are deployed to safeguard our infrastructure.

- **Physical security:** Access to data centres and corporate offices is controlled through secure entry systems, surveillance, and visitor management protocols.

- **Monitoring and logging:** Systems are continuously monitored, and user activities, exceptions, and security events are logged to help detect and respond to anomalies promptly.

- **Incident response:** A formal incident response plan ensures rapid containment, investigation, and remediation of security incidents.

- **Vendor management:** Third-party providers undergo security assessments and must comply with contractual obligations, including encryption and data protection standards.

- **Regular audits and risk assessments:** Internal audits and vulnerability assessments are conducted to identify and mitigate risks proactively.

From time to time, we may temporarily support older encryption standards to allow customers using legacy clients to migrate to our service. Our services may also support unencrypted, plain text access methods. If you choose to use these methods or weaker encryption standards, your data may be exposed in ways outside our control. We strongly recommend configuring your clients to use modern encryption standards, including TLS 1.2 or higher, for all access to our platforms.

These measures are supported by ongoing staff training, documented policies (e.g. Data Classification, Acceptable Use, and Password Management), and independent audits to align with recognised information security standards, including ISO/IEC 27001, and applicable data protection laws.

11. Children's privacy

We do not knowingly collect or solicit personal data from children or anyone under the age of eighteen (18). Please contact us if you believe we might have any personal data from or about a child or person under the age of eighteen (18). Our services are intended for customers aged eighteen (18) or over, and during sign-up we ask you to confirm that you are at least eighteen (18) years of age.

12. Direct marketing

While you are our customer, we may use your personal data from time to time to send you promotional material and direct marketing communications and information in relation to our products and services which we consider may be of interest to you. We do this by email, SMS, or other electronic messages or written notices, or through posting of such material on our services or our websites.

Where permitted by applicable law, we may send you direct marketing as an existing customer. In some countries, this means we can send you information about similar products or services because you are already our customer. Where the law requires your consent, we will obtain it before we send direct marketing.

Opt-out options. You can opt out of receiving direct or electronic marketing communications from us at any time by using the opt-out facilities provided in the marketing communications or by contacting us at privacy@themessaging.co

Please note that opting out of our marketing does not mean you will not be served advertisements online from third-party websites or in messages that may appear in your mailbox. You may still see advertisements based on your browsing history, or untargeted advertisements, but you will not be

served advertising nor be marketed to by us. We do not share personal data with any third party for their own marketing purposes.

13. Cookies

Our Cookie Policy at https://themessaging.co/cookie-policy provides you with information about how we collect, use, and disclose personal data through cookies.

We set non-essential cookies only with your consent, and we provide an easy way for you to change or withdraw that consent at any time. For further information, please see our Cookie Policy.

Google Analytics

We use Google Analytics to understand how people use our website. This involves cookies that collect information about your browsing activity. You can opt out of Google's advertising features through your Google account settings, browser add-ons, or your device's privacy settings. Google provides various tools and options to control how your data is used for advertising purposes. You can learn more about how Google uses your data and your available options on Google's privacy pages.

14. Third-party links

Our websites may include links to other websites or applications provided by others, including those acting on our behalf. We are not responsible for the practices employed by websites or services linked to or from our services or websites, including the information or content contained therein. Clicking on those links or enabling those connections may allow third parties to collect or share data about you in accordance with their own privacy policies.

Your browsing and interaction on any third-party website or service, including those with a link or advertisement on our websites, are subject to that third party’s privacy policies. You acknowledge that we do not control third-party websites, and we are not responsible for their privacy practices or policies. You should review the privacy policy of any third party and any applicable terms of use when you use their websites and applications.

15. Social media widgets

Our websites may include social media features (such as a Facebook Like button and/or other widgets) that run on our websites. These features may collect your IP address and which page(s) you visit on our websites and may set a cookie to enable the feature to function properly. Social media features and widgets are either hosted by a third party or hosted directly on our websites. Your interactions with these features are governed by the privacy policy of the organisation providing it.

16. Contact us

If you have any questions or concerns about your privacy, you may contact us via:

Data Controller: The Messaging Company Pty Ltd (ACN 669 674 382), Level 18, 324 Queen St, Brisbane, QLD, 4000, Australia

Data Protection Officer (DPO): Damien Vandooren dpo@themessaging.co

Privacy Enquiries: privacy@themessaging.co

17. Changes to our Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our practices, legal requirements, or for other operational reasons. The date of the most recent update will always be shown at the top of this Notice.

Where changes are material, we will notify you in advance (e.g. by email or by posting a clear notice on our website) before the changes take effect.

Our Privacy Notice can be viewed online at https://themessaging.co/privacy

Part B

Your region

Part B tells you, by country, which data protection law applies to you, who your regulator is, whether a local representative has been appointed, which transfer mechanism we rely on, and which regional supplement in Part C applies to you.

Country	Data protection law	Regulator	Representative	Transfer mechanism	Regional part
Australia	Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs)	Office of the Australian Information Commissioner (OAIC)	Not required	APP 8	**C1**
United Kingdom	UK GDPR and the Data Protection Act 2018	Information Commissioner's Office (ICO)	Cranium 8 Northumberland Ave London WC2N 5BY United Kingdom privacy@themessaging.co	UK International Data Transfer Agreement (IDTA) / Addendum	**C2**
EU / EEA	EU GDPR	Local supervisory authority	Cranium Excelsiorlaan 43/3 1930 Zaventem Belgium privacy@themessaging.co	EU Standard Contractual Clauses (SCCs)	**C3**
Isle of Man	Isle of Man Data Protection Act 2018	Isle of Man Information Commissioner	Cranium 8 Northumberland Ave London WC2N 5BY United Kingdom privacy@themessaging.co	Adequacy / SCCs	**C4**

Part C

Regional terms

The following regional terms apply to individuals in the relevant region and supplement Part A. Where a regional term conflicts with the core notice, the regional term prevails for individuals in that region.

C1. Australia

For individuals in Australia, the processing of your personal data is governed by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). The relevant privacy regulator is the Office of the Australian Information Commissioner (OAIC).

Your rights. Under the Privacy Act 1988 (Cth) and the Australian Privacy Principles, you may request access to the personal data we hold about you (APP 12) and request correction of that personal data (APP 13). You may also make a complaint about our handling of your personal data. Where we rely on our legitimate interests in the core notice, in Australia that processing is undertaken as permitted under the Australian Privacy Principles.

AU representative. A local representative is not required.

Transfers. Where we disclose your personal data to an overseas recipient, we handle that cross-border disclosure in accordance with Australian Privacy Principle 8 (APP 8), taking reasonable steps to ensure the recipient does not breach the APPs in relation to that information, or otherwise relying on the exceptions available under APP 8.

Automated decision-making: In line with Australian Privacy Principle 1, section 5 of this Privacy Notice outlines what automated decisions are made with computer programs that could affect your account or service. If you have a concern about an automated decision, you can contact us at privacy@themessaging.co

Right to complain. If you believe that we have breached the Australian Privacy Principles or otherwise mishandled your personal information, you may make a complaint to us by contacting us via privacy@themessaging.co and providing sufficient details about your complaint so that we can investigate. We will review your complaint and respond within a reasonable period. We aim to respond within thirty (30) days. If you are not satisfied with our response, or if we do not respond within thirty (30) days, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

C2. United Kingdom

Overseas transfers

Where we store and access your information

Your personal data may be stored, processed, or accessed in countries outside the United Kingdom, including where our service providers, technology providers, or other business partners are located or operate.

This may occur, for example:

- Where our service providers are based, or our technology infrastructure is located, outside the United Kingdom;
- When we work with overseas business partners;
- When we use cloud-based services or data storage solutions; or
- Where a transfer is required by law or legal proceedings.

Our approach to overseas transfers

Where UK data protection law applies and we transfer your personal data outside the United Kingdom, we ensure that the transfer is made in accordance with applicable data protection law. Depending on the circumstances, this may include:

- Transferring personal data to a country, territory or organisation covered by UK adequacy regulations;
- Putting in place appropriate safeguards to protect your personal data; or
- Relying on another lawful transfer mechanism or exception where permitted by applicable data protection law.

What this means for you

We take reasonable steps to ensure that personal data transferred outside the United Kingdom remains appropriately protected and that recipients:

- Process personal data only for authorised purposes;
- Apply appropriate technical and organisational security measures;
- Comply with applicable contractual and legal data protection obligations; and
- Assist us, where required, in responding to requests relating to your data protection.

Children’s personal data

We do not offer our service to, or knowingly collect or process personal data from, persons under the age of eighteen (18).

If we become aware that we have collected personal data from someone under eighteen (18) years of age, we will take reasonable steps to delete it.

If you are a parent or guardian and believe your child under the age of eighteen (18) has provided us with personal data, please contact us using the details provided in this Privacy Notice.

Data retention

How long we keep your information

We only keep your personal data for as long as we need it to:

- Provide our services to you;
- Meet our legal, tax, accounting or regulatory obligations; or
- Handle any complaints or legal issues that may arise.

We may keep your information for longer periods if:

- You make a complaint that we need to investigate or respond to;
- We reasonably believe legal action involving our relationship with you might occur; or
- The law requires us to keep it for specific timeframes.

How we decide retention periods

When determining how long to keep your information, we consider:

- How much information we have and how sensitive it is;
- The risk of harm if the information was accessed without permission;
- Whether we can achieve our purposes in other ways;
- What legal, regulatory, tax, or accounting rules require; and
- The nature of our relationship with you and the services we provide.

What happens when we no longer need your information

Once we no longer need your personal data, we will securely delete or anonymise it in accordance with our data retention policies and legal requirements.

Cookies and analytics

Cookies and pixels

We use cookies and similar tracking technologies on our website to enhance your browsing experience and improve our services.

Types of cookies we use

- Essential cookies: Necessary for the website to function properly.
- Performance cookies: To help us understand how visitors interact with our website.
- Functionality cookies: To remember your preferences and settings.

- Marketing cookies: To deliver relevant advertisements and track campaign effectiveness.

Cookie consent

When you first visit our website, you will see a cookie notice pop-up explaining our use of cookies. You can choose which types of cookies to accept and learn more about the cookies we use.

Managing your preferences

You can visit our Cookie Policy for detailed information about specific cookies, and change your cookie preferences at any time by adjusting your browser settings to refuse or delete cookies. Please note that disabling certain cookies may affect the functionality of our website and your user experience.

Your rights. Under the UK GDPR, you have the following rights in relation to your personal data:

- **Access** - to request a copy of the personal data we hold about you.
- **Rectification** - to request correction of any inaccurate or incomplete personal data.
- **Erasure** - to request deletion of your personal data where there is no lawful basis for us to continue processing it.
- **Restriction** - to request restriction of processing of your personal data in certain circumstances.
- **Portability** - to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another data controller.
- **Objection** - to object to processing of your personal data where we rely on legitimate interests as our lawful basis.
- **Withdraw consent** - where processing is based on your consent, you may withdraw that consent at any time.

Right to object. You have the right to object at any time, on grounds relating to your particular situation, to processing of your personal data which is based on our legitimate interests. Where you exercise this right, we will no longer process your personal data for those purposes unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise, or defence of legal claims.

UK representative. We have appointed Cranium, 8 Northumberland Ave, London, WC2N 5BY, United Kingdom, as our representative in the United Kingdom under Article 27 of the UK GDPR. You may contact our UK representative via privacy@themessaging.co in relation to matters concerning our processing of your personal data.

Automated decisions and AI. We may use artificial intelligence and/or automated processing tools to help deliver our services and protect our customers. Where we make such decisions, the rules in the Data (Use and Access) Act 2025 apply.

Making a complaint

If you're unhappy with how we've used your personal data, please get in touch with us first using the contact details at the end of this Privacy Notice. When you contact us:

- Give us as much detail as possible about your complaint and we will acknowledge your complaint within thirty (30) days of receiving it. If you contact us through social media, we will ask for an alternative secure contact method.
- We will investigate your complaint without undue delay. We will review all relevant facts, speak to relevant staff, and check that we have followed our own policies and standards. The time this takes depends on the complexity and scale of the issue and any harm you are suffering.
- We may contact you for more information if we are not sure what your complaint is about or to ask what outcome you are looking for. This helps us resolve your complaint more quickly.
- We will keep you updated on progress throughout our investigation. We will provide you with updates on timeframes, explain any delays, give you an expected completion date, and provide a point of contact for any questions.

Right to complain. If you are not satisfied with our response to your complaint, you have the right to make a complaint directly to the Information Commissioner's Office (ICO), the UK's data protection regulator, at any time.

The ICO's address:

Information Commissioner's Office
4th Floor, No.3 Circle Square
5 Hawkshaw Street
Manchester
M1 7BL
Helpline number: 0303 123 1113
Website: https://www.ico.org.uk/make-a-complaint

You don't have to contact us first before going to the ICO, but we'd appreciate the opportunity to try to resolve your concerns directly with you.

C3. European Union / European Economic Area

For individuals in the European Union / European Economic Area (EU/EEA), the processing of your personal data is governed by the EU GDPR, and your regulator is your local supervisory authority.

Your rights. Under the EU GDPR, you have the following rights in relation to your personal data:

- **Access** - to request a copy of the personal data we hold about you.
- **Rectification** - to request correction of any inaccurate or incomplete personal data.
- **Erasure** - to request deletion of your personal data where there is no lawful basis for us to continue processing it.
- **Restriction** - to request restriction of processing of your personal data in certain circumstances.

- **Portability** - to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another data controller.

- **Objection** - to object to processing of your personal data where we rely on legitimate interests as our lawful basis.

- **Withdraw consent** - where processing is based on your consent, you may withdraw that consent at any time.

Right to object. You have the right to object at any time, on grounds relating to your particular situation, to processing of your personal data which is based on our legitimate interests. Where you exercise this right, we will no longer process your personal data for those purposes unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise, or defence of legal claims.

EU representative. We have appointed Cranium, Excelsiorlaan 43/3, 1930 Zaventem, Belgium, as our representative in the European Union under Article 27 of the EU GDPR. You may contact our EU representative via privacy@themessaging.co in relation to matters concerning our processing of your personal data.

Transfers. Where we transfer your personal data outside the EEA to a country that is not covered by a European Commission adequacy decision, we rely on the EU Standard Contractual Clauses (SCCs) approved by the European Commission, and, where relevant, the Swiss Addendum. For transfers to the United States, we rely on the EU-US Data Privacy Framework where the recipient is certified.

Automated decisions and AI. We use computer programs, including AI, to make or help make some decisions about your account and messages, as described in section 5. Where such a decision is made solely by automated means and has a legal or similarly significant effect on you, Article 22 of the EU GDPR applies. In that case you have the right to obtain human intervention, to express your point of view and to contest the decision.

Right to complain. You have the right to lodge a complaint with the data protection supervisory authority in the EU/EEA Member State where you live or work, or where you believe that your rights have not been properly respected.

C4. Isle of Man

For individuals in the Isle of Man, the processing of your personal data is governed by the Isle of Man Data Protection Act 2018 (which applies the GDPR as part of the law of the Isle of Man), and your regulator is the Isle of Man Information Commissioner.

Your rights. Under the Isle of Man Data Protection Act 2018, you have rights in relation to your personal data corresponding to those set out in the core notice, including the rights of access, rectification, erasure, restriction, portability, objection (including the standalone right to object to processing based on our legitimate interests), and to withdraw consent.

Representative. We have appointed Cranium, 8 Northumberland Ave, London, WC2N 5BY, United Kingdom, as our representative in the United Kingdom under Article 27 of the UK GDPR. You may contact our UK representative via privacy@themessaging.co in relation to matters concerning our processing of your personal data.

Transfers. Where we transfer your personal data outside the Isle of Man, we rely on adequacy determinations where available, and otherwise on EU Standard Contractual Clauses (SCCs) and, where relevant, the Swiss Addendum.

Automated decisions and AI. The Isle of Man Data Protection Act 2018 applies the GDPR, including its restrictions on solely automated decision-making. Where any such decision producing legal or similarly significant effects concerning you is made, we apply the safeguards required, including meaningful human review and a way for you to contest the outcome.

Right to complain. You have the right to lodge a complaint with the Isle of Man Information Commissioner if you believe that your data protection rights have not been properly respected.