# Privacy Policy

Version 2026-10-17 · Effective 17 October 2026

Permanent link: tactful.ai/privacy-policy/2026-10-17

Tactful Ltd · Company No 10279888 · The Venture Centre, Stirling House, Cambridge Innovation Park, Denny End Road, Waterbeach, Cambridge, United Kingdom, CB25 9PB

## Section 1: Introduction and Scope

**1.1** This policy describes Tactful Ltd's commitment to protecting privacy when using Tactful Engage or successor products as specified in the Order Form.

**1.2** The policy covers: controller information, data types collected, usage purposes, third-party disclosures, international transfers, security measures, retention, and your legal rights.

### Controller Information

- **Company:** Tactful Ltd (Private Limited Company)
- **Registration:** England, Company No. 10279888
- **Address:** The Venture Centre, Stirling House, Cambridge Innovation Park, Denny End Road, Waterbeach, Cambridge, United Kingdom, CB25 9PB
- **Data Protection Authority:** UK Information Commissioner's Office, Registration No. ZA277573
- **Contact:** privacy@tactful.ai

**Policy Updates:** Last updated October 17, 2026. Changes will be notified via product or email.

## Section 2: Data Collection

### Types of Personal Data Collected

- **Contact Data:** Name, identification number, email, telephone
- **Correspondence Data:** Records of communication and survey responses
- **Anti-fraud Data:** Financial information, creditworthiness, transaction details, identity documents
- **Payment Data:** Card and payment information
- **Technical Data:** IP address, login data, usage information
- **User Credentials:** Usernames and passwords
- **Usage Data:** Product usage details
- **Marketing and Communications Data:** Marketing preferences

### Collection Methods

Personal data is collected through:

- Third parties (directly)
- Cookies (per Cookie Policy on tactful.ai)
- Direct interactions: registration, product use, marketing requests, correspondence

- Social media (Facebook, WhatsApp, and others)
- Public sources
- Third-party analytics providers

**Failure to Provide Data:** Where data is legally required or contractually necessary, failure to provide it may prevent contract performance.

### Aggregated Data

Aggregated statistical or demographic data is collected for monitoring and developing the Product. This data does not identify individuals and is not considered personal data. However, combining aggregated data with personal data makes it subject to this policy.

## Section 3: Personal Data Usage

Personal data is used where it is necessary to perform contracts with you, necessary for our legitimate interests (balancing your rights), or required for legal compliance.

| Purpose | Data Types | Legal Basis |
|---|---|---|
| **Registration** | Contact Data | Contract performance; Legitimate interests |
| **Communication** — Responding to queries, support, relationship management, surveys | Contact Data, Correspondence Data, User Credentials, Marketing and Communications Data | Contract performance; Legitimate interests; Legal obligations |
| **Payment** — Processing orders, managing payments, debt recovery | Contact Data, Correspondence Data, Transaction Data, Payment Data | Contract performance; Legitimate interests |
| **Fraud Prevention** — Investigating and preventing fraud; may share with fraud prevention agencies | Anti-fraud Data, Contact Data, Correspondence Data, Transaction Data, Payment Data | Legal obligations; Legitimate interests |
| **Product Operation** — Delivery, login generation, troubleshooting, maintenance, support, hosting | Contact Data, Correspondence Data, User Credentials, Technical Data, Usage Data | Contract performance; Legal obligations; Legitimate interests |
| **Analysis of User Requirements** — Understanding service requirements, business analysis, product development | Contact Data, Correspondence Data, User Credentials, Usage Data, Marketing and Communications Data | Legitimate interests |
| **Marketing** | Contact Data, Correspondence Data, User Credentials, Usage Data, Technical Data, Marketing and Communications Data | Consent (for direct marketing via email, push, SMS). Right to withdraw per Section 8. |
| **Content Delivery** — Effective content presentation; may share with partners and service providers | Contact Data, Correspondence Data, User Credentials, Usage Data, Technical Data, Marketing and Communications Data | Legitimate interests |

## Section 4: Third-Party Disclosures

Personal data may be shared with:

| Third Party | Purpose |
|---|---|
| Group members | Administration of group operations |
| Service providers | Hosting, advertising, marketing |
| Professional advisors | Consulting, legal, banking, audit, insurance, accounting |
| HM Revenue & Customs | Reporting of processing activities |
| Potential purchasers | In connection with business sale |

## Section 5: International Transfers

**5.1** Personal data may be accessed, transferred, or stored outside the UK or European Economic Area, including the United States.

**5.2** The supplier safeguards personal data as described in this policy.

**5.3** Appropriate safeguards meeting UK/EU GDPR requirements are implemented, including:

- UK International Data Transfer Agreement (IDTA)
- EU Commission Standard Contractual Clauses
- UK Extension to the EU-US Data Privacy Framework, for providers certified under it
- Supplementary measures as needed

**5.4** Contact the supplier for information on specific transfer mechanisms.

## Section 6: Security Measures

**6.1** Appropriate security measures prevent accidental loss, unauthorized access, alteration, or disclosure.

**6.2** Access is limited to employees, agents, contractors, and third parties with a business need.

**6.3** Representatives process data only on instructions and are subject to confidentiality duties.

**6.4** Procedures are in place for suspected breaches; notification is provided as legally required.

**6.5** No data transmission over the Internet can be guaranteed to be secure from intrusion, but the supplier maintains commercially reasonable physical, electronic, and procedural safeguards.

**6.6** Data is stored and accessed subject to security policies and standards.

**6.7** Users are responsible for keeping passwords confidential and complying with security procedures.

## Section 7: Data Retention

**7.1** Retention periods are based on business needs and legal obligations (legal, regulatory, tax, accounting, reporting requirements).

**7.2** Data is retained only as long as necessary for processing purposes and related permissible purposes.

**7.3** Longer retention applies if a complaint is filed or litigation is reasonably anticipated.

**7.4** Retention determination considers: amount, nature, and sensitivity of data; risk of harm from unauthorized use or disclosure; whether purposes are achievable through other means; and applicable legal, regulatory, tax, and accounting requirements.

**7.5** When no legitimate business need remains, the supplier will either irreversibly anonymise data (and may further retain and use it) or securely destroy it.

## Section 8: Your Legal Rights

**8.1** Contact the supplier using the details in Section 1 for questions about personal data use.

**8.2** Under certain conditions, you have the following rights:

| Right | Description |
|---|---|
| **Request Access** | Require the supplier to provide copies of personal data held about you |
| **Request Correction** | Require updates to inaccuracies in personal data |
| **Request Erasure** | Request deletion of data the supplier no longer has the right to lawfully use |
| **Object to Processing** | Object to processing based on legitimate interests (unless overriding grounds exist) |
| **Request Restriction** | Suspend processing to: establish data accuracy; address unlawful use; retain for legal claims; or verify overriding grounds |
| **Request Transfer** | Transfer data in a structured, machine-readable format to third parties (applies to automated data provided with consent or used for contract performance) |
| **Withdraw Consent** | Stop particular processing activities based on consent |

**8.3** Rights are subject to exemptions safeguarding public interest (crime prevention) and supplier interests (legal privilege).

**8.4** The supplier responds within one month in most cases.

**8.5** Withdrawal of consent may prevent access to certain products or services.

**8.6** There is no fee to access data or exercise rights; however, a reasonable fee may apply for unfounded, repetitive, or excessive requests.

**8.7** If unsatisfied, you have the right to complain to the UK ICO or the competent supervisory authority in your country of residence.

**UK Information Commissioner's Office:** ico.org.uk