



TomCRM Data Processing Agreement

Between TomCRM Limited and the Customer

Customer: [Customer name]
TomCRM-DPA-001 Rev 1 | September 2026

Commercial in confidence. This agreement forms part of the TomCRM service terms between the parties and may not be used for any other purpose without the written permission of TomCRM Limited.

Parties and effective date

This Data Processing Agreement (the Agreement) is made between:

(1) TomCRM Limited, company number 15662063, registered in England and Wales, whose registered office is at 128 City Road, London EC1V 2NX, registered with the Information Commissioner's Office under reference ZB691927 (TomCRM, the Processor); and

(2) [Customer name], company number [number], whose registered office is at [address] (the Customer, the Controller).

Effective date: [date], or the date the Customer's TomCRM account is first made available to it, whichever is earlier.

This Agreement relates to the TomCRM subscription and any trial, set-up, support, integration or backup service that TomCRM provides to the Customer (the Services), under which TomCRM configures, supports and maintains a CRM and automation account for the Customer on the HighLevel platform. It sets out the terms on which TomCRM processes personal data on the Customer's behalf and forms part of the agreement between the parties for the Services (the Principal Agreement). The Principal Agreement is the TomCRM Service Level Agreement: Software Services (TomCRM-SLA-004) signed or accepted by the Customer, including its Schedules and any Change Order, or, during a free trial, the TomCRM trial agreement signed by the Customer, which applies TomCRM-SLA-004 to the trial.

1. Definitions and roles

Terms used in this Agreement have the meanings given to them in the UK GDPR and the Data Protection Act 2018 unless defined otherwise here. "Data Protection Laws" means the UK GDPR, the Data Protection Act 2018 and any other data protection law that applies. "UK GDPR" means the retained EU General Data Protection Regulation as it forms part of the law of England and Wales. "Sub processor" means any third party engaged by TomCRM to process the Customer's personal data. "Platform" means the HighLevel software on which the Services are delivered.

For the personal data processed under the Services, the Customer is the controller and TomCRM is the processor. The Customer decides why and how the personal data is processed. TomCRM processes it only on the Customer's behalf and on its instructions, as set out in this Agreement. The details of the processing are in Schedule 1.

2. Processing on documented instructions

TomCRM will process the Customer's personal data only on the Customer's documented instructions, including in relation to transfers of personal data, unless required to do otherwise by law. This Agreement and the Principal Agreement are the Customer's initial documented instructions. The Customer's use of the account, including the automations, campaigns, integrations and Ai features it switches on, is a further documented instruction for the processing those features involve. If TomCRM is required by law to process personal data beyond those instructions, it will tell the Customer before doing so unless the law prohibits it.

If TomCRM considers that an instruction infringes Data Protection Laws, it will tell the Customer without undue delay.

3. TomCRM's obligations as processor

TomCRM will:

- **Documented instructions.** process the personal data only as set out in clause 2.
- **Confidentiality.** ensure that anyone authorised to process the personal data is subject to a duty of confidence, whether contractual or statutory.
- **Security.** take the technical and organisational measures required by Article 32 of the UK GDPR, as set out in Schedule 3.
- **Sub processors.** engage sub processors only in line with clause 7.
- **Data subject rights.** assist the Customer, by appropriate technical and organisational measures, to respond to requests from data subjects exercising their rights. The account gives the Customer direct access to view, correct, export and delete contact records, so most requests can be handled by the Customer without TomCRM's involvement.
- **Wider assistance.** assist the Customer with security, breach notification, data protection impact assessments and prior consultation, as set out in clauses 9 and 10.
- **Return and deletion.** return or delete the personal data at the end of the Services, as set out in clause 12.
- **Records and audits.** make available the information needed to demonstrate compliance with this Agreement and allow for and contribute to audits, as set out in clause 13.

4. The Customer's obligations as controller

The Customer confirms that it has a lawful basis for the processing it instructs, that it has provided any privacy information required to data subjects, and that it has obtained any consents needed, including for marketing communications by email and SMS under the Privacy and Electronic Communications Regulations. The Customer's instructions to TomCRM will comply with Data Protection Laws. The Customer is responsible for the accuracy, quality and lawfulness of the personal data it enters or imports, for the content of the communications it sends through the account, for managing its own users and their permissions, and for not entering special category data or data about children unless clause 6 and Schedule 1 have been updated to cover it.

5. Confidentiality

TomCRM keeps the personal data confidential and limits access to those members of its team and its sub processors who need it to provide the Services. Anyone with access is bound by confidentiality obligations and has appropriate data protection awareness.

6. Security measures

TomCRM puts in place and maintains the technical and organisational measures set out in Schedule 3 to protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, taking account of the state of the art, the costs of implementation, and the nature, scope and purposes of the processing, as well as the risk to data subjects. Where the Customer intends to process special category data or data about children, the parties will agree any additional measures in writing and record them in Schedule 1 before that data is entered.

7. Sub processors and support access

The Customer gives general authorisation for TomCRM to engage the sub processors listed in Schedule 2. TomCRM will impose data protection obligations on each sub processor that are equivalent to those in this Agreement, and remains responsible to the Customer for each sub processor's performance. TomCRM will tell the Customer at least 30 days before adding or replacing any sub processor, giving the Customer the opportunity to object on reasonable data protection grounds. If the parties cannot resolve an objection, the Customer may terminate the Services affected and clause 12 applies.

The Platform is provided by HighLevel Inc., which is TomCRM's principal sub processor. HighLevel's own sub processors (including its cloud hosting, messaging and Ai providers) are engaged under HighLevel's Customer Data Processing Addendum, which gives 30 days' notice of changes and a right of objection, and are listed at gohighlevel.com/sub-processors. TomCRM will pass on any such notice it receives.

Support access. TomCRM's staff access the Customer's account only to set it up, provide support, investigate faults and maintain it, and only to the extent needed for that purpose. HighLevel may also access the account for support and security purposes under its terms with TomCRM. Both kinds of access are processing on the Customer's documented instructions under this Agreement, are covered by the confidentiality obligations in clause 5, and are logged by the Platform.

8. Artificial intelligence processing

The Platform includes Ai features (for example conversation assistants, content generation, call summaries and voice agents) which process personal data only when the Customer switches them on. Where the Customer enables an Ai feature, the processing is carried out by HighLevel and its Ai providers as sub processors under Schedule 2, on the Customer's instruction. Neither TomCRM nor, under its DPA, HighLevel uses the Customer's personal data to train models for other customers. TomCRM will tell the Customer which Ai features are enabled in its account on request and will help the Customer assess a feature before it is switched on where the Customer asks. Separately, TomCRM staff may use the Ai assistant listed in Schedule 2 to read and draft support correspondence and to help configure the Customer's account; that use is covered by the confidentiality obligations in clause 5, is subject to the provider's commercial terms under which customer data is not used to train models, and a person at TomCRM reviews anything it produces before it is sent or applied.

TomCRM carries out no solely automated processing that produces legal or similarly significant effects on a data subject. Any automated decision the Customer configures in its own workflows is the Customer's decision as controller.

9. Assistance to the Customer

Taking account of the nature of the processing and the information available to it, TomCRM will assist the Customer in meeting its obligations to keep personal data secure, to notify and communicate personal data breaches, to carry out data protection impact assessments, and to consult the Information Commissioner's Office where required. Much of the technical information the Customer needs for a data protection impact assessment, including the data flows, sub processors, security measures and the Ai data handling, is set out in this Agreement, its schedules and the TomCRM Security and Continuity Statement (TomCRM-RPT-001), which TomCRM provides on request.

TomCRM is not the Customer's Data Protection Officer and does not act in that role. Each party is responsible for designating its own data protection contact, recorded in Schedule 4.

10. Personal data breaches

TomCRM will notify the Customer without undue delay, and in any event within 24 hours, of becoming aware of a personal data breach affecting the Customer's personal data, and will provide the information and assistance set out in Schedule 4. HighLevel is required under its DPA to notify TomCRM within 72 hours of becoming aware of a suspected breach on the Platform, and TomCRM's 24 hours runs from that notification. The Customer, as controller, is responsible for deciding whether to notify the Information Commissioner's Office and any affected data subjects. TomCRM records all personal data breaches.

11. International transfers

The Platform is hosted in the United States, so the Customer's personal data is transferred outside the United Kingdom as part of the Services. That transfer is made under HighLevel's Customer Data Processing Addendum, which incorporates the UK standard contractual clauses, and HighLevel is certified under the UK Extension to the EU-US Data Privacy Framework. Support may also be provided from India by HighLevel's affiliate under the same clauses. TomCRM will not make any other transfer of the Customer's personal data outside the United Kingdom or the European Economic Area except where an appropriate safeguard applies, such as an adequacy decision, the UK International Data Transfer Agreement or standard contractual clauses, or on the Customer's documented instruction. The safeguard relied on for each sub processor is shown in Schedule 2.

12. Return and deletion of data

The Customer can export its contacts, opportunities, form submissions and appointments from the account as CSV files at any time. On termination of the Services, the Customer may export its data, or ask TomCRM for a full export, for 30 days (the Export Period). At the end of the Export Period, or earlier if the Customer asks in writing, TomCRM will securely delete the Customer's account and any copies TomCRM holds, unless retention is required by law, and will confirm deletion in writing on request. Copies held in the Platform's backups are overwritten on its rolling seven-day backup cycle. Records deleted by the Customer during the Services are recoverable from the Platform's recycle bin for 30 days and are then permanently deleted. Where the Customer takes the monthly backup add-on, the archive copies are deleted at the same time or handed to the Customer, as the Customer chooses.

13. Records and audit

TomCRM will make available to the Customer the information reasonably needed to demonstrate compliance with this Agreement, including the Platform's current ISO/IEC 27001 certificate, its SOC report and its security documentation. The Customer may audit TomCRM's compliance on reasonable written notice, normally no more than once a year, and additionally following a personal data breach. Audits are conducted so as to cause minimal disruption, and any information obtained is treated as confidential. Audits of the Platform itself are satisfied by HighLevel's independent certifications and reports, which TomCRM will obtain for the Customer on request. Each party bears its own costs of an audit, except that where the Customer requires an on-site audit, more than one audit in a year other than following a personal data breach, or an audit of HighLevel beyond its published reports, the Customer pays TomCRM's reasonable costs, including any charge HighLevel makes, at the rates in the Principal Agreement.

14. Liability

Each party's liability arising out of or in connection with this Agreement is subject to the limitations and exclusions of liability in clause 17 of the Principal Agreement, including the separate cap for data protection claims in clause 17.4 of TomCRM-SLA-004. Nothing in this Agreement limits any liability that cannot be limited by law, or either party's liability to data subjects or to the Information Commissioner under Data Protection Laws.

15. Term, termination and survival

This Agreement takes effect on the Effective Date and continues for as long as TomCRM processes personal data on the Customer's behalf under the Services, including any trial. The clauses concerning confidentiality, return and deletion of data, audit and liability survive termination for as long as TomCRM holds any of the Customer's personal data or as long as needed to give them effect.

16. Governing law and precedence

This Agreement is governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales. If there is a conflict between this Agreement and the Principal Agreement on the processing of personal data, this Agreement prevails, except on liability, which is governed by clause 14 of this Agreement and clause 17 of the Principal Agreement.

17. Signatures

Signed for and on behalf of the parties by their authorised representatives. Where the Customer accepts the Principal Agreement online when signing up, this Agreement is incorporated by that acceptance and a countersigned copy is provided on request.

For the Customer (Controller)	For TomCRM Limited (Processor)
Name:	Name: Tommy Findlay
Position:	Position: Director
Signature:	Signature:
Date:	Date:

Schedule 1: Details of the processing

Item	Detail
Subject matter	The processing of personal data needed for TomCRM to provide, configure, support and maintain the Customer's CRM and automation account (the Services), including any trial period.
Duration	For the term of the Services, including any trial, and until all personal data is returned or deleted under clause 12.
Nature and purpose	Hosting, storage, organisation, structuring, retrieval, transmission, automation and erasure of personal data within the Customer's TomCRM account, so that the Customer can record enquiries and contacts, manage a sales pipeline, send email and SMS communications, take bookings, run web forms and automate follow-up. TomCRM accesses the account only to set it up, support it and maintain it on the Customer's instruction.
Categories of data subjects	The Customer's prospects, leads, customers and their contacts; referrers and partners; the Customer's own staff and users of the account; and, where the Customer chooses to put them in the system, other individuals the Customer deals with.
Categories of personal data	Names, email addresses, phone numbers, postal addresses, job titles and organisations; enquiry and conversation history (email, SMS, call recordings and voicemail where the Customer enables them); pipeline stage, notes, tags and custom fields the Customer defines; appointment details; form submissions; marketing preferences and consent records; and records of user activity in the account (audit logs).
Special category data	The Services are not designed for special category data (for example health data) or for data about children, and the Customer must not enter such data unless the parties have agreed it in writing beforehand and Schedule 1 has been updated to record the safeguards. Criminal offence data is not processed.

Schedule 2: Sub processors

TomCRM uses the following sub processors to provide the Services. TomCRM will tell the Customer at least 30 days before adding or replacing any sub processor.

Sub processor	Purpose	Location	Safeguard
HighLevel Inc.	The CRM and automation platform on which TomCRM is delivered: hosting, storage, messaging, calendars, forms, automations and platform Ai features. HighLevel may access the account for support and security purposes under its terms.	United States (Google Cloud Platform and Amazon Web Services); support also from HighLevel India Pvt. Ltd	HighLevel Customer Data Processing Addendum incorporating UK standard contractual clauses; certified under the UK Extension to the EU-US Data Privacy Framework; ISO/IEC 27001:2022; SOC 2 Type II

Sub processor	Purpose	Location	Safeguard
HighLevel's own sub processors	Messaging (Twilio, Mailgun), payments (Stripe), Ai features (OpenAI and other Ai providers), analytics and support tooling, as listed at gohighlevel.com/sub-processors	United States unless stated on that list	Flowed down under HighLevel's DPA; 30 days' notice of changes
Make.com (Celonis)	Only where the Customer commissions an integration or automation that runs outside the platform	European Union	Provider DPA; standard contractual clauses
Hetzner Online GmbH	Only where the Customer takes the monthly backup add-on: runs the scheduled job that exports the Customer's data from the Platform	Germany (Nuremberg)	Provider DPA; EU hosting
Supabase	Only where the Customer takes the monthly backup add-on: encrypted archive copy of exports for 12 months	United Kingdom (London)	Provider DPA; UK or EU hosting
iS3 Ltd	Configuration, integration and support work carried out for TomCRM by iS3 staff, under a written agreement with TomCRM	United Kingdom	Written processing terms equivalent to this Agreement
TSLTD Limited	Sales, onboarding, configuration and support work carried out for TomCRM by Tom Stansfield, under a written agreement with TomCRM	United Kingdom	Written processing terms equivalent to this Agreement
Google (Workspace)	TomCRM's business email and documents, used when the Customer sends support requests, exports or data files to TomCRM	United States and European Union	Google Cloud Data Processing Addendum; UK standard contractual clauses
Anthropic PBC (Claude Team plan)	Ai assistance used by TomCRM staff to read and draft support email and to help configure accounts; customer data is not used to train models under Anthropic's commercial terms	United States	Anthropic commercial terms and Data Processing Addendum; UK standard contractual clauses

Not TomCRM sub processors: any system the Customer connects to its account itself (for example its own Google Workspace or Microsoft 365, its website, its accounting or payment provider) is contracted directly by the Customer, which holds its own data protection terms with that provider. Where the Customer takes the monthly backup add-on, the Google Drive or OneDrive folder the exports are delivered to is the Customer's own.

Schedule 3: Technical and organisational security measures

The measures below combine those of the Platform, which are independently assessed under ISO/IEC 27001:2022 and SOC 2 Type II, and those TomCRM applies to its own access and operations. They are reviewed and updated as the Platform and the risks change.

Encryption

Personal data is encrypted in transit using TLS 1.2 or later and encrypted at rest using AES-256, with keys held in a managed key management system and rotated.

Access control

Access to the Customer's account is by named user accounts with role-based permissions set by the Customer. Two-factor authentication is available and is enforced for TomCRM staff accounts and, on request, for the Customer's users. TomCRM staff access is limited to least privilege and removed when no longer needed. The Platform records user activity in audit logs.

Hosting and resilience

The Platform runs on Google Cloud Platform and Amazon Web Services across multiple availability zones and virtual private cloud networks, with DDoS mitigation and a web application firewall. A public status page reports Platform health.

Backups

Platform databases are backed up daily with seven days of backups retained, and web, application and database components are deployed with point in time recovery. Records deleted in error are recoverable for 30 days. Where the Customer takes the monthly backup add-on, a dated export is delivered to a folder the Customer owns and a second encrypted copy is retained by TomCRM for 12 months, with a quarterly restore check.

Vulnerability management and testing

The Platform runs automated vulnerability scanning and annual third-party penetration testing, and applies security patches under its ISO 27001 controls. TomCRM keeps any integration it builds for the Customer up to date and applies patches in good time.

Personnel

Anyone at TomCRM with access to personal data is bound by confidentiality obligations, has appropriate data protection awareness, and is granted only the access they need. TomCRM is led by an IRCA-qualified ISO 27001 lead auditor and ISO 42001 lead implementer.

Data minimisation and retention

Only the personal data needed for the Services is processed. The Customer controls what is entered and can delete records at any time; data is deleted at the end of the Services under clause 12.

Supplier management

Sub processors are subject to due diligence and to written terms that impose obligations equivalent to those in this Agreement. HighLevel's certifications are reviewed on renewal and its sub processor notices are passed on to the Customer.

Schedule 4: Personal data breach process

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

TomCRM will notify the Customer without undue delay, and in any event within 24 hours, of becoming aware of a personal data breach affecting the Customer's personal data. The notification will include, so far as it is known at the time:

- the nature of the breach, including the categories and approximate number of data subjects and records affected
- the likely consequences of the breach
- the measures taken or proposed to address it and to limit any harm
- a contact point for further information

Where TomCRM cannot provide all of this at once, it will provide information in phases without further undue delay. The Customer, as controller, is responsible for deciding whether to notify the Information Commissioner's Office within 72 hours and whether to notify affected data subjects. TomCRM will assist the Customer with both.

Response steps

1. Detect and triage the issue, including any notification received from HighLevel.
2. Contain it and stop any ongoing exposure, for example by suspending a user, an integration or an automation.
3. Assess the scope and the risk to data subjects.
4. Notify the Customer within the time above.
5. Support the Customer's investigation and any notifications.
6. Remediate, then record the breach and the lessons learned.

Contacts

TomCRM (Processor)	Customer (Controller)
Tommy Findlay tommy@is3.co.uk 01522 287318	[Name] [Email] [Phone]