Datacrazy Platform Privacy Policy

1. Who we are and to whom this Policy applies

CRM DATACRAZY LTDA., registered with the Brazilian National Register of Legal Entities (CNPJ) under number 54.129.748/0001-18, with its registered office at Avenida Osmar de Souza Nunes, 220, Dos Pioneiros, Balneário Camboriú/SC, postcode (CEP) 88.331-070 ("Datacrazy", "we", "us"), develops and operates a CRM platform for customer service, automation and relationship management through channels such as WhatsApp and Instagram (the "Platform").

This Policy explains how we process personal data, in compliance with the Brazilian General Data Protection Law (Law No. 13.709/2018, "LGPD"), the Brazilian Internet Civil Framework (Marco Civil da Internet, Law No. 12.965/2014) and other applicable rules. It applies to:

- **Visitors** to our Site (datacrazy.io and its subdomains);
- **Leads and prospective customers** who fill in forms, book demos, take part in events or talk to our sales team;
- **Customers** (contracting individuals or legal entities) and their **Users** (people authorised to access the Platform);
- Datacrazy **Affiliates**;
- **Data subjects whose data is entered into the Platform by our Customers** (for example, the Customers' end customers, leads and WhatsApp and Instagram contacts), within the limits described in Section 2.

Capitalised terms not defined here have the meaning given to them in the Terms of Use.

2. Our roles: controller and processor

The LGPD distinguishes between the party that makes decisions about the processing (the **controller**) and the party that processes data on behalf of another (the **processor**). Datacrazy acts in **both roles**, and this determines who is responsible for what.

Situation	Datacrazy's role	Who decides and is accountable to the data subject
Data of visitors, leads and affiliates, and the registration, billing and usage data of Customers and Users	Controller	Datacrazy
Data that the Customer enters, imports, collects or receives through the Platform (contacts, WhatsApp and Instagram conversations, deals, notes, files, custom fields)	Processor	The Customer, which is the controller

2.1. As controller, Datacrazy determines the purposes and means of the processing and is responsible for it in accordance with this Policy.

2.2. As processor, we process the Customer's data **solely** to provide the Platform, following the Customer's instructions (the Terms of Use and the settings chosen by the Customer). We do not use this data for our own purposes, we do not sell it and we do not use it for advertising. We may only use Platform usage data in aggregated and anonymised form, without identifying the Customer or the content of its messages, for statistics, security and service improvement. The Customer is responsible for having a legal basis to process the data, informing its own data subjects, obtaining consent where necessary

and responding to requests from those data subjects.

2.3. If you are a data subject whose data is held in the database of one of our Customers and you wish to exercise your rights, please contact the Customer first. If you contact us, we will forward the request to the Customer and assist it in handling the request, as described in Section 13.

3. What data we process

3.1. Data you provide to us

- **Registration and account:** name, email, telephone number, job title, company, CNPJ, country, profile photo (optional), time zone, language and access credentials (the password is stored in protected form, never in plain text).
- **Forms, demos, events and surveys:** data you provide, such as name, email, telephone number, company, company size and interest.
- **Contact and support:** content of messages and requests, attachments, contact information and support history.
- **Payment and billing:** name or corporate name, tax identification document, billing address, payment method and status and the **last four digits** of the card. Full card details are processed directly by the payment provider and **are not stored by us**.
- **Testimonials and reviews:** name, job title, company and content, only with your authorisation.
- **Affiliates:** registration and commercial data of the affiliate and its representatives.

3.2. Data collected automatically

- **Technical and device data:** IP address, browser type and version, operating system, language, screen resolution, device identifiers, pages visited, referring URL, and dates and times of access.
- **Platform usage data:** features accessed, clicks, frequency and duration of use, settings, errors, performance metrics and storage volume.
- **Access logs and acceptance records:** kept in accordance with the Marco Civil da Internet and the Terms of Use, and for security and audit purposes.
- **Cookies and similar technologies:** as described in Section 5 and in our Cookie Policy.
- **Email trackers** (open and click pixels) in marketing communications, where permitted by law and by your preferences. You can disable them by blocking images from loading in your email program.

3.3. Data received from third parties

- **Meta and connected channels:** when WhatsApp, Instagram, Messenger or other channel accounts are connected, we receive, through Meta's official API or through third-party integrations chosen by the Customer, the data needed for operation, such as account identifiers, contacts' numbers and profile names, messages, media and delivery metadata.
- **Payment providers:** billing status, payment confirmation and payment default data.
- **Affiliates and event organisers:** referrals and contact details of people who have expressed interest, including at events organised in partnership.

3.4. Customer data processed as processor

The Customer decides what data to enter. It usually includes the identification and contact details of end customers and leads, conversation content, audio, images, documents and sales history. Datacrazy does not control this content and does not access it, except where necessary to provide the service, provide support requested by the Customer, ensure security or comply with the law.

3.5. Sensitive personal data

We do not request sensitive data (Article 5(II) of the LGPD), such as data concerning health, racial or ethnic origin, religious or political beliefs, biometrics or sex life. **We ask the Customer to avoid entering such data into the Platform**, including in the AI features. If the Customer needs to process such data, it is the Customer's responsibility to have a specific legal basis (Article 11 of the LGPD), and the Customer must inform us so that we can assess the appropriate additional measures.

4. What we use data for and on what legal bases

Purpose	Examples	Legal basis (LGPD)
Creating and maintaining the account, authenticating access and providing the Platform	Registration, login, permissions, backups	Performance of a contract or of preliminary procedures (Article 7(V))
Billing, invoicing and tax obligations	Issuing invoices, reconciliation, management of payment defaults	Contract (Article 7(V)), legal obligation (Article 7(II)) and credit protection (Article 7(X))
Technical support and customer service	Resolving tickets, analysing failures	Contract (Article 7(V)) and legitimate interest (Article 7(IX))
Security and prevention of fraud and abuse	Detecting suspicious access, blocking spam, auditing	Legitimate interest (Article 7(IX)) and credit protection (Article 7(X)), where applicable
Compliance with legal and regulatory obligations; retention of access logs	Marco Civil da Internet, requests from authorities	Legal obligation (Article 7(II))
Regular exercise of rights	Records of acceptance, defence in judicial, administrative or arbitration proceedings, payment disputes	Article 7(VI)
Product improvement and development	Usage statistics, testing, bug fixing	Legitimate interest (Article 7(IX)), using aggregated or anonymised data whenever possible
Operational communications	Security notices, renewal, billing, changes to the Terms, incidents	Contract (Article 7(V)) and legal obligation (Article 7(II))
Marketing, newsletters, events and B2B sales prospecting	Emails, WhatsApp, invitations, event reminders, rich content materials	Consent (Article 7(I)) or legitimate interest (Article 7(IX)), as the case may be, always with an option to unsubscribe
Satisfaction surveys and feedback	NPS, post-event surveys, user interviews	Legitimate interest (Article 7(IX))
Negotiating and entering into contracts with affiliates	Affiliate registration and contracts	Performance of a contract or of preliminary procedures (Article 7(V))
Non-essential cookies, measurement and advertising	Analytics, remarketing, conversion attribution	Consent (Article 7(I))
Corporate transactions	Due diligence, merger, acquisition	Legitimate interest (Article 7(IX)) and regular exercise of rights (Article 7(VI))

When we rely on **legitimate interest**, we take into account your legitimate expectations and your fundamental rights and freedoms (Article 10 of the LGPD) and respect your right to object. When we rely on **consent**, you may withdraw it at any time, without affecting the processing carried out before the withdrawal.

We process your data only for purposes compatible with those stated here. If a new, incompatible purpose arises, we will inform you and, if necessary, ask for your consent again.

5. Cookies and tracking technologies

We use cookies and similar technologies (browser local storage, pixels, tags and session recording) in the following categories:

- **Strictly necessary:** the basic operation and security of the Site, such as storing your cookie preferences and keeping the session active. These do not depend on consent.
- **Functional:** embedded features, such as the calendar for booking demos and video playback.
- **Analytics and performance:** understanding how the Site is used so we can improve it.
- **Advertising and marketing:** measuring campaigns, attributing conversions, rewarding affiliates and showing relevant ads.

Non-essential cookies are **disabled by default** and are only enabled after you give your consent, which you can manage at any time through the banner or the **"Cookie preferences"** link in the Site footer. You can also block cookies in your browser, but some features may stop working. The cookies used, their providers, purposes and retention periods are detailed in our Cookie Policy.

6. Artificial intelligence

The Platform offers AI features (Crazy IA), such as customer service agents, response suggestion and generation, conversation summaries and lead classification. With regard to these features:

- **The Customer's role:** the Customer is the controller of the data processed by these features and decides whether and how to enable them. Datacrazy processes this data as processor.
- **No model training:** Datacrazy **does not train AI on Customer data**, whether inputs, messages, files or other content.
- **AI providers:** the features are run by AI model providers engaged on an API basis, whose terms do not allow this data to be used for training. The data may be processed temporarily by these providers, including outside Brazil (Section 9).
- **Automated decisions:** Datacrazy does not make decisions based solely on automated processing that produce legal effects or significantly affect data subjects. Data subjects may request a review of decisions made solely on the basis of automated processing and information on the criteria used, subject to commercial and industrial secrecy (Article 20 of the LGPD).
- **Transparency:** a Customer that sets up agents that automatically reply to its contacts must disclose that the service is automated whenever the law or good faith so requires.

7. Who we share data with

We do not sell personal data, nor do we share it with third parties for advertising purposes in exchange for payment. We share only what is necessary, in the cases below or with your consent.

7.1. Categories of recipients

- **Infrastructure and service providers (sub-processors):** cloud hosting and storage, email, payment processing, anti-fraud, customer service, usage analytics, messaging and AI. They may only process data in accordance with our instructions and under contracts containing confidentiality, security and data protection obligations.

- **Meta and other channel platforms** (WhatsApp, Instagram, Messenger and third-party integrations chosen by the Customer): when the Customer connects these channels, data passes through these platforms, which have their own policies. See Section 8.
- **Integrations chosen by the Customer:** ERPs, payment methods (such as Stripe), automation tools, calendars and other applications that the Customer connects, including via Webhook, REST API and MCP Server.
- **Datacrazy Affiliates:** where the data subject has expressed an interest in subscribing through an affiliate, or where the Customer is served by an affiliate with access authorised by the Customer.
- **Companies in the same economic group**, if any, solely for the purposes of this Policy.
- **Professional advisers:** lawyers, auditors, accountants and insurers, subject to a duty of confidentiality.
- **Public authorities:** where there is a legal obligation, a court order or a valid request, or for the regular exercise of rights and fraud prevention. We assess the lawfulness and scope of the request before complying.
- **Financial institutions and card schemes:** in payment disputes (chargebacks), the evidence of the subscription and of use, in accordance with the Terms of Use.
- **Corporate transactions:** in a merger, acquisition, demerger or sale of assets, the data may be transferred to the successor, which will be bound by this Policy. We will notify data subjects of significant changes.

7.2. Anonymised and aggregated data

We may share aggregated statistics and anonymised data (which do not allow you to be identified, taking into account reasonable technical means) for research, reporting and corporate marketing purposes.

7.3. Sub-processors

The Customer authorises Datacrazy to engage sub-processors, such as cloud, AI and messaging providers, which may be located outside Brazil, in compliance with Articles 33 to 36 of the LGPD. Information about sub-processors may be requested through the channel in Section 15.

8. WhatsApp, Instagram and other third-party integrations

As a CRM integrated with messaging channels and other applications, the Platform depends on services that we do not control. Therefore:

- **Meta:** the use of WhatsApp, Instagram and Messenger is also governed by Meta's terms and policies. The Customer is responsible for complying with them, including the rules on opt-in, message templates, prohibited content and customer service windows. Datacrazy may suspend integrations that breach these rules or put the account of the Customer or of other customers at risk.
- **WhatsApp connection methods:** WhatsApp may be connected through Meta's official API (official provider) or through third-party integrations chosen by the Customer. In the latter case, conversation data also passes through these third parties, which have their own policies, and the Customer assumes the risks of that choice, in accordance with the Terms of Use.
- **Opt-in and bulk communications:** the Customer must have a legal basis and, where required, the prior consent of recipients before sending messages, and must respect blocking and unsubscribe requests. Sending unsolicited communications is prohibited.
- **Permissions:** by connecting an integration, the Customer authorises access to the data of the connected account, which may include reading, writing and changing information. We recommend

carefully reviewing the permissions granted. Datacrazy is not responsible for the privacy and security practices of third parties, nor for failures or unavailability of their services.

- **Data held by providers:** data stored by the providers themselves (such as conversation history within WhatsApp) is governed by those providers' policies.

9. International data transfers

Personal data is stored and processed in **Brazil** and in the **United States of America**, where some of our providers are located, including cloud, AI, and analytics and advertising tool providers. For transfers outside Brazil, we will adopt one of the mechanisms provided for in Article 33 of the LGPD and in the ANPD's regulations, such as:

- transfer to a country or international organisation with an adequate level of protection recognised by the ANPD;
- **standard contractual clauses** approved by the ANPD, or other safeguards provided for by law;
- other applicable legal grounds, such as specific and prominent consent, where necessary.

You may request more information about the safeguards adopted through the channel in Section 15.

10. How long we keep data

We keep data only for as long as necessary for the stated purposes, subject to legal time limits. At the end of that period, we delete or anonymise the data, except in the cases of retention provided for in Article 16 of the LGPD.

Category	Retention period
Account data and Customer Data (conversations, contacts, files)	For as long as the contract is in force. After the Account is closed, the Customer has 90 days to export its data; after that, the data is held in restricted retention for a further 60 days, with no access by the Customer, and is permanently deleted from the active database within 30 days, unless there is a legal obligation to retain it. Backup copies follow the rule below
Backup copies (backups)	Kept until overwritten by the regular backup cycle (see below)
Application access logs	6 months, in accordance with Article 15 of the Marco Civil da Internet
Records of acceptance, charges and communications	Until the end of the applicable limitation period, for the regular exercise of rights
Lead and prospect data	For as long as necessary for the purpose, or until you request deletion or object to the processing
Preferences and records of consent and opt-out	For the period necessary to demonstrate compliance with your choice, even after you unsubscribe. The record of cookie choices is kept for 12 months
Data for defence in disputes or subject to a court or authority order	Until the end of the limitation period or the period set by the authority

Backup copies. We keep backup copies (backups) to ensure the integrity and availability of data and to allow recovery in the event of an incident, as part of the security measures required by Article 46 of the LGPD. Due to technical limitations, it is not possible to delete individual records from these copies. Therefore, when data is deleted from the active database, it may remain in backup copies until they are overwritten by the regular backup cycle. During that period, the copies are stored securely, with restricted access, are not used for any other purpose and are only accessed to recover data in the event of an incident.

11. How we protect your data

We adopt technical and administrative measures capable of protecting personal data against unauthorised access and against accidental or unlawful destruction, loss, alteration, communication or dissemination.

The provider responsible for payment processing also adopts its own security measures.

No system is completely immune to risk. Therefore, **Customers and Users also have responsibilities**: keeping their credentials and API tokens confidential, using strong passwords, enabling two-factor authentication where available, granting access only to those who need it, revoking the access of former staff and keeping their devices secure. Notify us immediately through the official channels if you suspect unauthorised access.

12. Security incidents

In the event of a security incident that may result in significant risk or harm to data subjects:

- **Data processed as processor:** we will notify the Customer within **72 hours** of confirmation of the incident, with the information available so that it can fulfil its obligations as controller, including towards the ANPD and the data subjects.
- **Data processed as controller:** we will notify the ANPD and the affected data subjects within the time limit set by the ANPD's regulations, describing the nature of the data affected, the data subjects involved, the security measures used, the related risks, the reasons for any delay and the measures taken to reverse or mitigate the effects.

13. Your rights and how to exercise them

You may request, at any time and upon request, under Article 18 of the LGPD:

1. **Confirmation** of the existence of processing;
2. **Access** to the data;
3. **Correction** of incomplete, inaccurate or out-of-date data;
4. **Anonymisation, blocking or deletion** of unnecessary or excessive data or data processed in breach of the law;
5. **Portability** to another provider, in accordance with the ANPD's regulations;
6. **Deletion** of data processed on the basis of consent, except in the cases of retention provided for by law;
7. **Information about sharing** with public and private entities;
8. **Information about the possibility of not giving consent** and about the consequences of refusing;
9. **Withdrawal of consent**;
10. **Objection** to processing carried out on a legal basis other than consent, in the event of non-compliance with the law, and, at any time, to receiving direct marketing;
11. **Review** of decisions made solely on the basis of automated processing that affect your interests;
12. **Petition** to the National Data Protection Authority (ANPD) and consumer protection bodies.

How to make a request: by email to dpo@datacrazy.io, stating the right you wish to exercise.

Identity verification: for your security, we may ask for additional information to confirm that you are the data subject or their legal representative. We will not fulfil requests that we cannot verify, in order to prevent unauthorised access to third parties' data.

Time limit: confirmation of existence or access in simplified format will be provided immediately, where possible. The full statement will be provided within 15 days of the valid request (Article 19 of the LGPD), or within the time limits set by the applicable regulations.

Limitations: we may refuse or limit the request where there is a legal or regulatory obligation to retain the data, a need for the regular exercise of rights, or where fulfilling it would require the disclosure of commercial or industrial secrets or of third parties' data. When this happens, we will explain the reason.

Data controlled by Customers: if your data is in the database of a Datacrazy Customer, the Customer is responsible for handling your request. If you contact us, we will forward the request to the Customer, without handling it directly, unless instructed by the Customer or required by law.

Marketing opt-out: use the unsubscribe link in marketing emails or write to the channel in Section 15. We will continue to send essential communications, such as security, billing and renewal notices and contractual changes.

Exercising your rights is free of charge, and you will not suffer any discrimination for exercising them.

14. Children and adolescents

The Platform and the Site **are not intended for persons under 18 years of age**. By registering, you declare that you are 18 years of age or older. Datacrazy does not knowingly collect or request personal data from persons under 18.

If we find that an account belongs to a person under 18 or that we have collected personal data of a child or adolescent without the specific consent of their legal guardians, where required, we will close the account and promptly delete that data, except in the cases of mandatory retention provided for by law. Parents or guardians may contact us through the channel in Section 15.

A Customer that, in the course of its operations, processes data of children and adolescents is solely responsible for complying with Article 14 of the LGPD and the specific legislation, including the assessment of the data subject's best interests.

15. Data Protection Officer (DPO) and contact

For questions, requests, complaints or to exercise your rights:

- **Data Protection Officer (DPO):** Andreone Souza Ribeiro, dpo@datacrazy.io
- **Address:** Avenida Osmar de Souza Nunes, 220, Dos Pioneiros, Balneário Camboriú/SC, CEP 88.331-070

If you are not satisfied with the response, you may lodge a complaint with the **ANPD** (www.gov.br/anpd) and with other competent bodies.

16. Customers' responsibilities

By using the Platform, the Customer, as controller of the data it enters or collects, declares and undertakes to:

- have an appropriate legal basis for each processing operation and purpose, and obtain valid consent whenever necessary;
- inform its data subjects about the use of the Platform and of processors such as Datacrazy, maintaining its own privacy policy;
- collect only the data that is necessary and **not enter sensitive data** without a specific legal basis and prior notice to Datacrazy;

- respect opt-out, blocking and unsubscribe requests, and not send unsolicited or bulk communications in breach of the law and of the policies of Meta and other providers;
- respond to data subject requests, with reasonable support from Datacrazy;
- keep its Users and permissions up to date and be responsible for activities carried out with its credentials and tokens;
- not use the Platform for unlawful, discriminatory or fraudulent purposes, nor to process data obtained illegitimately, such as lists purchased without a legal basis;
- notify Datacrazy of any incident affecting the data processed on the Platform.

Failure to comply with these obligations may lead to the suspension or closure of the Account, without prejudice to other measures, and Datacrazy may exercise its right of recourse under the law and the Terms of Use.

17. Third-party links and content

Our Site and the Platform may contain links, embedded videos and calendars, widgets and social media features from third parties. These third parties may collect data about your interaction and have their own policies, which we recommend you read. Datacrazy is not responsible for their practices.

18. Changes to this Policy

We may update this Policy to reflect legal, regulatory or technical changes or changes to our services. The current version will always be available at legal.datacrazy.io/privacy-policy/en, with the date of the last update, and previous versions remain available. Significant changes will be communicated by email or on the Platform. If a change requires consent, we will request it again.

19. Governing law

This Policy is governed by the laws of the Federative Republic of Brazil. The rights of consumers and data subjects provided for by law remain guaranteed, including the right to bring proceedings in the courts of their place of domicile where the law so provides.