GDPR Compliance Statement

GDPR

TROOTH, LLC GDPR-2026-001

Document Title	GDPR Compliance Statement
Document ID	GDPR-2026-001
Version	2.0
Classification	Public
Effective Date	September 18, 2026
Next Scheduled Review	March 18, 2027
Document Owner	D'Andre Heggie, Founder and Sole Member
Entity	Trooth, LLC
Supersedes	GDPR Compliance Statement 1.0, June 8, 2026 (signed)
Reference Frameworks	Regulation (EU) 2016/679 (GDPR); UK GDPR; AICPA TSC (Security, Confidentiality, Privacy)

1. Executive summary

This statement sets out how Trooth, LLC meets its obligations under the General Data Protection Regulation, in both of the roles it holds: controller of the personal data of the people who hold Trooth accounts and who correspond with the Company, and processor of the personal data a customer submits to the Trooth Network under that customer's instructions. It names the lawful basis for each purpose, how a data subject exercises each right and in what time, where data rests and on what transfer mechanism, and what the Company does within seventy-two hours of learning of a breach. It also states plainly what the Company has not done: it has appointed no representative in the Union under Article 27, and it is not required to appoint a Data Protection Officer under Article 37.

2. Scope

Trooth, LLC (the Company) operates one product: the Trooth Network, a web application at trooth.co with a public API at api.trooth.co. A company connects its systems, the Network records what is true of them on a schedule with the source and the time of each observation, and buyers read that record. This statement covers that product, the production database that holds its data, the deployment pipeline that builds it, and the administrative accounts the Company holds with each provider named in its published Sub-processor List. It does not cover preview or development environments, which hold no customer data. As at the effective date the Company has no employees or contractors; every requirement written for personnel applies to the Founder today and to every future person from their first day.

3. The two roles

Role	Whose personal data	Governed by
Controller	Account holders and workspace members: name, work email, authentication records, session and security events, product usage. People who write to the Company: address and the content of the message.	This statement and the Privacy Policy at trooth.co/privacy
Processor	Personal data inside the records a customer creates in the Network: contacts named on a company profile, the addresses a buyer request is sent to, the people named in a document a company shares, the recipients of a notification the workspace configures.	The Data Processing Addendum at trooth.co/dpa, incorporated into the customer terms without negotiation

The Company does not determine the purpose of the personal data a customer places in its own workspace, and does not use that data for any purpose of its own. It does not sell personal data, does not share it for cross-context behavioural advertising, and does not use customer content, connected-integration data or account information to train any model.

4. Lawful bases, by purpose

Purpose	Lawful basis	Article
Creating and operating an account; delivering the Network to the person who asked for it	Performance of a contract	6(1)(b)

Purpose	Lawful basis	Article
Authentication, session security, rate limiting, bot protection, fraud and abuse prevention	Legitimate interests: keeping the service and its users safe	6(1)(f)
Recording material actions in an append-only audit ledger so a record cannot be altered silently	Legitimate interests, and performance of a contract where the record is the product	6(1)(f), 6(1)(b)
Service and security email a person cannot opt out of without closing the account	Performance of a contract	6(1)(b)
Optional subscriptions: product updates, status notices, Trust Center updates	Consent, given by double opt-in and withdrawable in one click	6(1)(a)
Answering a message sent to the Company	Legitimate interests, or consent where the person volunteered the detail	6(1)(f), 6(1)(a)
Meeting a legal obligation, and establishing or defending a legal claim	Legal obligation; legitimate interests	6(1)(c), 6(1)(f)

The Company processes no special category data under Article 9 and no criminal offence data under Article 10, and the Network is not built to receive either. It performs no automated decision-making producing legal or similarly significant effects on a person within the meaning of Article 22: the Network's AI-assisted features draft, and a person makes every decision that binds a company or a buyer.

5. Data subject rights

Right	Article	How it is exercised	Time
Access, and a copy of the data	15	privacy@trooth.co, or the account's own export	30 days
Rectification	16	In the product, or privacy@trooth.co	30 days; usually immediately in the product

Right	Article	How it is exercised	Time
Erasure	17	Closing the account, or privacy@trooth.co	30 days from live systems; backups expire on a 30-day rolling window
Restriction of processing	18	privacy@trooth.co	30 days
Portability	20	privacy@trooth.co, or the account's own export, in a machine-readable format	30 days
Objection, including to processing on legitimate interests	21	privacy@trooth.co	30 days
Withdrawal of consent	7(3)	The unsubscribe link in any optional email, in one click	Immediately
Complaint to a supervisory authority	77	Directly to the authority; the Company asks for, but does not require, the chance to answer first	Set by the authority

A request is answered within thirty days and free of charge. Identity is confirmed against the account before data is released; where the Company cannot identify a person from the data it holds, it says so under Article 11 rather than collecting more data to look. Where the Company acts as processor, a request that reaches it is passed to the customer who controls that data within five business days and the Company assists that customer under Article 28(3)(e). The erasure path is exercised against the live database on every build, not only described here.

6. International transfers

- Primary customer data rests in the United States, in AWS us-east-1, through Neon. The Company offers no other residency region on the effective date and says so rather than implying otherwise.
- Transfers of personal data out of the European Economic Area and the United Kingdom are made on the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) and, for the United Kingdom, the International Data Transfer Addendum, both incorporated by the Data Processing Addendum at trooth.co/dpa.
- Every sub-processor is listed publicly with its purpose and its processing region at trooth.co/subprocessors, and customers receive thirty days' notice of a new one and may object for reasonable cause.

- A transfer impact assessment is recorded for each sub-processor that receives personal data outside the EEA, considering the destination's law, the data at issue and the technical measures below. It is available on request.

7. Security of processing, Article 32

Encryption in transit on every connection and at rest in the managed database and its backups; tenant separation enforced twice, in the application from the session and again in the database by row-level security under a role that cannot bypass it; an append-only, hash-linked audit ledger; multi-factor authentication available to every account; nightly encrypted backups with a monthly restore rehearsal; and one hundred and fifty-two automated gates that a change must pass before it can reach production. Each of these is stated control by control, with the evidence for it, on the published Trust Center at trooth.co/security, and the technical detail is in the Encryption in Transit and at Rest Assurance Statement (ATT-03) and the Network Architecture and Data Flow Disclosure (ATT-04).

8. Personal data breach

Where the Company acts as processor it notifies the affected customer without undue delay and within seventy-two hours of becoming aware, as the Data Processing Addendum commits, with what is known, what is not yet known, the likely consequences and the measures taken. Where it acts as controller it notifies the competent supervisory authority within seventy-two hours under Article 33 where the breach is likely to result in a risk to people, and the people themselves without undue delay under Article 34 where that risk is high. Incidents are classified into four severities with response times from fifteen minutes; the Incident Response Policy (POL-09) is published.

9. Accountability

Obligation	Position on the effective date
Records of processing activities, Article 30	Maintained. Available to a customer or an authority on request; a summary of purposes, categories, recipients and retention is in the Privacy Policy.
Data protection impact assessment, Article 35	One has been carried out for the Network's processing and is published (REG-01), although the Company's processing is not of a kind that requires one under Article 35(1).

Obligation	Position on the effective date
Data protection officer, Article 37	Not appointed, and not required: the Company's core activities do not consist of regular and systematic monitoring of data subjects on a large scale, nor of large-scale processing of special category data. privacy@trooth.co reaches the Founder, who is accountable for data protection.
Representative in the Union, Article 27	NOT APPOINTED. Whether Article 27 applies to the Company's processing is a question the Founder has recorded for counsel; the published Trust Center states this control as not in place rather than leaving it out.
Processor engagement, Article 28	Every sub-processor is engaged under a written data processing agreement, within the purpose and region published, and is reviewed as the Vendor and Third-Party Risk Management Policy (POL-14) requires.
Data protection by design and by default, Article 25	The Network collects what a purpose needs and no more; a new mutating route cannot ship without a declared request schema, and a new table cannot ship without a row-level security policy.

10. Contact

privacy@trooth.co for any matter in this statement, including a data subject request. security@trooth.co for a security report. Trooth, LLC is a Florida limited liability company, registration L25000561494, in Miami, Florida, United States.

Reference: Regulation (EU) 2016/679 Articles 5, 6, 12-22, 25, 27, 28, 30, 32-35, 37, 44-49. Related: Privacy Policy (trooth.co/privacy); Data Processing Addendum (trooth.co/dpa); Sub-processor List (trooth.co/subprocessors); Data Retention Summary (trooth.co/retention); POL-09 Incident Response; POL-11 Backup and Data Retention; POL-14 Vendor and Third-Party Risk Management; POL-18 Data Residency; ATT-03; ATT-04; REG-01 Data Protection Impact Assessment.

Authorization

This statement is issued by Trooth, LLC under the authority of its Founder and Sole Member and describes the Company as it operates on its effective date. It is a published statement of the Company and requires no signature to bind it; the version published at trooth.co/security is the current one, and an earlier version, including any signed version of June 8, 2026, is superseded in full. It is not a certification and not an audit opinion: Trooth holds no audited certification against any framework and does not represent otherwise. Where this statement and the live service disagree, the service is corrected or the statement is re-issued, and the Company's published Trust Center states, control by control, what is in place and what is not.