Privacy Policy

for thetaloop.app and the research service "ThetaLoop CSP Research"

Version: April 2026

1. Controller

Controller within the meaning of the General Data Protection Regulation (GDPR) and other national data protection laws of the Member States as well as other data protection provisions is:

Carsten Hasenstab IT Dienstleistungen
Owner: Carsten Hasenstab
c/o Impressumservice Dein-Impressum
Stettiner Strasse 41
35410 Hungen, Germany
VAT ID: DE424472679
E-mail: thetaloopsignals@gmail.com

The address stated above is an address for service provided via a commercial imprint service (§ 5 DDG, German Digital Services Act). For data protection supervision, the authority at the place of central administration of the controller is competent pursuant to Art. 55 GDPR in conjunction with § 40 BDSG (see Section 3).

2. Data Protection Officer

A data protection officer has **not** been appointed. No appointment obligation exists under § 38(1) BDSG (German Federal Data Protection Act), as the controller generally employs fewer than 20 persons continuously engaged in the automated processing of personal data, does not carry out any processing requiring a data protection impact assessment under Art. 35 GDPR, and does not conduct commercial data processing for the purpose of transmission, anonymized transmission or market or opinion research. Art. 37(1) GDPR also does not apply. For data protection inquiries, please contact the above address.

3. General Rights of Data Subjects and Competent Supervisory Authority

As a data subject, you have, under the GDPR, among others the following rights: access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), data portability (Art. 20), objection to certain processing (Art. 21) and the right to withdraw any consent given at any time with effect for the future (Art. 7(3)). For details see Section 14.

You also have the right to lodge a complaint with a supervisory authority (Art. 77 GDPR). The competent authority for the controller is:

Bavarian State Office for Data Protection Supervision (BayLDA)
Promenade 18, 91522 Ansbach, Germany
Postbox 1349, 91504 Ansbach
Tel.: +49 (0) 981 180093-0
E-mail: poststelle@lda.bayern.de
Web: https://www.lda.bayern.de

4. Website Visits to thetaloop.app — Server Logs

When our website is accessed, our hosting / CDN provider Cloudflare (see Section 5) automatically collects information transmitted by your browser to the server ("server logs"):

- IP address of the requesting device (in truncated or full form, depending on the Cloudflare configuration);

- date and time of the request;
- name and URL of the file requested;
- volume of data transferred, HTTP status code;
- user-agent (browser type and version, operating system);
- referrer URL.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in stability, security and abuse prevention).
Storage period: generally 30 days, after which the data is deleted or fully anonymized.

5. Cloudflare as Hosting Provider and CDN

Our website is delivered via the infrastructure of **Cloudflare, Inc.**, 101 Townsend Street, San Francisco, CA 94107, USA (together with its European subsidiaries). Cloudflare acts as a reverse proxy, CDN and DDoS-protection service. In doing so, Cloudflare processes technically necessary connection data such as IP address, HTTP headers, user-agent and, where applicable, request contents.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in a secure, performant and globally available delivery).

Transfer to the USA (third country): Cloudflare, Inc. is certified under the **EU-U.S. Data Privacy Framework (DPF)** (EU Commission adequacy decision of 10 July 2023, Implementing Decision (EU) 2023/1795; status confirmed by the General Court of the EU in Case T-553/23, Latombe v. Commission, on 3 September 2025). The legal basis for transfers to the USA is therefore primarily **Art. 45 GDPR** in conjunction with the DPF. In addition, the controller has concluded the **EU Standard Contractual Clauses (SCC)** with Cloudflare pursuant to Commission Implementing Decision (EU) 2021/914, which continue to apply even if the DPF status should change (Art. 46(2)(c) GDPR).

Further information: https://www.cloudflare.com/privacypolicy/

6. Cloudflare Web Analytics (cookieless reach measurement)

On the website, we use **Cloudflare Web Analytics** for aggregated, **cookieless** reach measurement. No cookies are set, no device-based identifiers are stored or read beyond what is strictly technically necessary, and no personal profiles are created. Only aggregated metrics on page views, referrers, device / browser classes and coarse regions are collected.

Legal basis under GDPR: Art. 6(1)(f) GDPR (legitimate interest in privacy-friendly, aggregated analysis of user behaviour).
§ 25 TDDDG (German Act on Data Protection and Privacy in Telecommunications and Telemedia): Since no information is stored in or read from the user's device beyond what is strictly necessary, no consent under § 25(1) TDDDG is required (§ 25(2) No. 2 TDDDG analogously).

7. No Cookies, No Third-Party Tracking

On the website, **no tracking cookies, no marketing cookies and no cookies for other profiling** are used. In particular, we do **not** use: Google Analytics, Google Tag Manager, Meta / Facebook Pixel, TikTok Pixel, LinkedIn Insight Tag, X / Twitter Pixel or comparable services. No cross-device recognition and no automated profiling for advertising purposes takes place.

8. Whop as Marketplace and Payment Platform

The subscription is purchased and billed via the platform of **Whop, Inc.**, 12 East 49th Street, 11th Floor, New York, NY 10017, USA ("Whop"). Whop operates the sales platform, administers accounts, routes payments and engages payment service providers. In this context, Whop processes in particular:

- account and master data (name, e-mail address, where applicable billing address, username);

- purchase and billing data;
- communication and support data;
- technical connection and log data.

Legal basis: Art. 6(1)(b) GDPR (performance of pre-contractual measures and contract performance); additionally Art. 6(1)(c) GDPR (tax and commercial retention obligations) and Art. 6(1)(f) GDPR (fraud prevention, IT security).

Transfer to the USA: For the transfer to Whop, Inc. in the USA, we rely on the **EU Standard Contractual Clauses (SCC)** pursuant to Art. 46(2)(c) GDPR in conjunction with Commission Implementing Decision (EU) 2021/914. A DPF certification of Whop, Inc. is not documented at present; the controller reviews the status regularly. The controller has additionally performed a Transfer Impact Assessment (TIA) and taken into account supplementary safeguards (transport encryption, data minimization).

Whop Privacy Policy: https://whop.com/privacy

9. Stripe as Payment Service Provider (sub-processor via Whop)

For card processing, Whop uses **Stripe, Inc.**, 354 Oyster Point Boulevard, South San Francisco, CA 94080, USA, and **Stripe Payments Europe, Ltd.**, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland. Stripe processes in particular payment instrument data (card / account information, transaction data, fraud prevention data). The controller has no direct access to this data; only billing / transaction confirmations are received.

Legal basis: Art. 6(1)(b) GDPR; additionally (c) and (f).
Transfer to the USA: Stripe, Inc. is certified under the **EU-U.S. Data Privacy Framework (DPF)** (Art. 45 GDPR). The **EU Standard Contractual Clauses** apply additionally (Art. 46(2)(c) GDPR).

Stripe Privacy Policy: https://stripe.com/privacy

10. Telegram Messenger as Delivery Channel (third-country transfer UAE / BVI)

Research content is delivered via the **Telegram** messenger, operated by **Telegram FZ-LLC**, Business Central Towers, Tower A, Office 1003/1004, Sheikh Zayed Road, P.O. Box 501919, Dubai, United Arab Emirates (UAE), and **Telegram Group Inc.**, P.O. Box 146, Road Town, Tortola, British Virgin Islands (BVI).

Data processed by the Provider: Telegram username and/or Telegram user-ID (strictly required to associate channel access with the paid subscription); where applicable, messages exchanged during support.

Data processed by Telegram itself: phone number, profile data, device and connection data, message content and metadata in accordance with Telegram's own privacy policy.

Legal basis for processing by the Provider: Art. 6(1)(b) GDPR (contract performance — without a Telegram identifier, delivery of the Service is not possible).

Transfer to the UAE / BVI: Neither the United Arab Emirates nor the British Virgin Islands are covered by an EU Commission adequacy decision. Enforceable EU Standard Contractual Clauses with Telegram are not practicable. Transfers are therefore additionally based on your **express consent** pursuant to **Art. 49(1)(a) GDPR**. Before the first transfer — at the latest during the checkout process or when linking your Telegram account — you will be expressly informed about the risks of such transfers and give your active opt-in consent. You may withdraw your consent at any time with effect for the future (Art. 7(3) GDPR); in that case, the Service can no longer be delivered and the contract may be terminated.

Known risks: Telegram currently does not have an EU representative appointed under Art. 27 GDPR. Supervisory authorities (among others the German Federal Commissioner for Data Protection (BfDI) and the Hamburg Data Protection Commissioner (HmbBfDI)) have raised data-protection concerns regarding Telegram; the enforcement of your data-subject rights vis-à-vis Telegram may be impeded.

Telegram Privacy Policy: https://telegram.org/privacy

11. Render (backend hosting)

For the backend (generation of research content, data processing, databases), the controller uses the services of **Render Services, Inc.**, 525 Brannan Street, Suite 300, San Francisco, CA 94107, USA. The backend application and databases used by the Provider are hosted on Render.

Data processed: predominantly internal logs, technical metrics, aggregated market data and internal process data. In principle, no direct customer master data is stored at Render; customer identification data remains at Whop. To the extent technically necessary for delivery, the Telegram user-ID may be processed.

Legal basis: Art. 6(1)(b) and (f) GDPR.
Transfer to the USA: Render Services, Inc. has been certified under the **EU-U.S. Data Privacy Framework (DPF)** since 6 January 2025 (Art. 45 GDPR). The **EU Standard Contractual Clauses** apply additionally as a fallback (Art. 46(2)(c) GDPR).

Render Privacy Notice: https://render.com/privacy

12. Market Data Providers

For the generation of research content, market data (such as prices, quotes, options chains and related exchange information) is obtained from licensed third-party market data providers as well as from publicly available market data sources. **No customer data** is transmitted to these providers; only market data requests without subscriber identification are triggered. No data-protection-relevant transfer of personal data takes place in this context.

13. No Automated Decisions, No Profiling

No **automated decision-making** within the meaning of Art. 22 GDPR takes place. No **profiling** of subscribers (for advertising, scoring or credit-assessment purposes) is carried out.

14. Rights of Data Subjects — Details

As a data subject, you have, in particular, the following rights:

- **Right of access (Art. 15 GDPR):** You may request information about the personal data concerning you as well as further information referred to in Art. 15 GDPR.
- **Right to rectification (Art. 16 GDPR):** You may request the correction of inaccurate or the completion of incomplete personal data concerning you.
- **Right to erasure (Art. 17 GDPR):** You may request the erasure of personal data concerning you, provided the statutory requirements are met and no legal retention obligations conflict.
- **Right to restriction of processing (Art. 18 GDPR)** under the conditions listed therein.
- **Right to data portability (Art. 20 GDPR):** You may receive the personal data concerning you, which you have provided to the controller, in a structured, commonly used and machine-readable format.
- **Right to object (Art. 21 GDPR):** You may object at any time, for reasons arising from your particular situation, to processing based on Art. 6(1)(e) or (f) GDPR.
- **Right to withdraw consent (Art. 7(3) GDPR):** Where processing is based on your consent (in particular for Telegram third-country transfers), you may withdraw it at any time with effect for the future, without affecting the lawfulness of processing based on consent prior to withdrawal.
- **Right to lodge a complaint with a supervisory authority (Art. 77 GDPR):** You may contact a data protection supervisory authority at any time, in particular the BayLDA (contact details see Section 3).

To exercise your rights, please contact the address stated in Section 1.

15. Retention Periods

• **Contract, accounting and billing data:** retained for the statutorily prescribed period (generally 10 years under § 257 HGB, § 147 AO — German Commercial Code and German Fiscal Code). After expiry, data is deleted unless further statutory retention obligations exist.

• **Server and access logs:** 30 days.

• **Communication (support messages):** until the matter is finally resolved, and thereafter in accordance with statutory retention periods.

• **Other data:** deleted as soon as the purpose of processing has been achieved and no statutory retention obligations conflict.

16. No Services for Persons Under 16

The Service is directed exclusively at persons of legal age or with full legal capacity. The Provider **does not collect data from persons under 16**. Should the Provider become aware of an unintended data processing involving a person under 16, the relevant data will be deleted without delay, unless a statutory retention obligation conflicts.

17. Data Security

The Provider implements technical and organizational measures (TOMs) in accordance with Art. 32 GDPR and the state of the art to protect data against unauthorized access, loss, alteration and other unauthorized processing. These include, in particular:

• transport encryption of all web connections via TLS (HTTPS);

• encrypted storage of passwords and sensitive configuration data;

• access restrictions to databases and production systems on a least-privilege basis;

• regular updates of the software used;

• logging of security-relevant events;

• conclusion of appropriate data-processing / third-country agreements (SCC / DPF) with all service providers.

18. Updates

The Provider reserves the right to adapt this Privacy Policy to changes in the applicable law, to changes in the Service or to changes in the third-party providers used. The version published at this location applies at any given time.

19. Version

This Privacy Policy is valid from **April 2026**.