



CONVERSAND PRIVACY POLICY

This Privacy Policy explains how Affluencer sp. z o.o. sp. k., with its registered office at 27 Stycznia 9, 34-120 Andrychów, Poland, entered in the Register of Entrepreneurs of the National Court Register under KRS No. 0000779028, tax No. NIP 6762563897 ("Affluencer", "Conversand", "we", "us"), processes personal data in connection with the Conversand affiliate network, our websites, the Interface and related services.

You can contact us at: mail@conversand.com.

1. Scope

This Privacy Policy applies to:

- publishers, advertisers, applicants and their authorised users;
- visitors of our websites and Interface;
- people who contact us or subscribe to communications;
- End Users who click affiliate links, interact with tracking technologies, visit advertiser properties or complete tracked actions;
- job candidates and business contacts.

This Privacy Policy should be read together with the Conversand General Affiliate Agreement, applicable Program Terms, cookie notices and any specific privacy notice displayed in the Interface.

2. Our role

For account administration, payments, fraud prevention, security, support, marketing and our own website analytics, Affluencer usually acts as an independent controller.

For affiliate tracking and conversion reporting, the role may differ by technical setup and Program. Affluencer, Advertisers and Publishers may act as independent controllers, joint controllers, processors or subprocessors. Where a separate data processing agreement or joint controller arrangement applies, it will supplement this Privacy Policy.

Publishers and Advertisers remain responsible for providing their own privacy notices and obtaining consents required for their websites, apps, channels and communications.

3. Personal data we process

3.1. Publisher, advertiser and account data

We may process:

- name, business name, job title, username and authorised user details;
- email address, phone number, postal address and communication preferences;
- account credentials, authentication data and login logs;
- company registration data, tax numbers, VAT status, tax residence and billing data;
- bank account, payment provider identifiers and payout data;

- traffic source information, website/app/channel URLs, social media handles, promotional methods and Program applications;
- performance data, click data, conversion data, commission data, invoices, statements and payment history;
- support messages, complaints, notices, audit records and correspondence;
- identity, sanctions, anti-fraud, KYC and compliance data where required;
- device, browser, IP address, Interface usage logs and security logs.

3.2. End User and affiliate tracking data

When an End User interacts with an Affiliate Link, Advertiser Program or tracking integration, we may process:

- IP address, approximate location, device type, browser type, operating system, language and time zone;
- cookie IDs, click IDs, impression IDs, device identifiers, advertising identifiers and similar online identifiers;
- referrer URL, landing page URL, publisher ID, subpublisher ID, program ID and advertiser ID;
- date and time of click, impression, visit, lead, sale or other Action;
- transaction ID, order ID, basket value, currency, product category, conversion status, return/cancellation status and validation data;
- postback, server-to-server and tag data sent by Advertisers or Publishers;
- fraud prevention signals, such as duplicate patterns, velocity, abnormal traffic, proxy/VPN indicators, bot indicators and quality scores.

We normally do not need an End User's name, email address, postal address or payment card data for affiliate tracking. If an Advertiser or Publisher sends such data to Conversand, it must have a valid legal basis and comply with applicable law and Program Terms. Where possible, data should be pseudonymised or minimised.

3.3. Website visitors and contacts

We may process contact form data, email content, newsletter subscription data, analytics data, cookies, IP address, device data and information about interactions with our website.

3.4. Recruitment data

If you apply for a job or cooperate with us in recruitment, we may process your CV, contact details, employment history, education, qualifications, portfolio, interview notes, salary expectations and other information you provide.

3.5. Special category data

We do not intentionally request special category data, such as health, biometric, genetic, political, religious or trade union data, unless a specific legal basis applies. Please do not provide such data unless requested and lawful.

4. How we collect data

We collect data:

- directly from you when you register, use the Interface, contact us, complete forms or provide documents;

- automatically through the Interface, cookies, pixels, logs, APIs, postbacks and similar technologies;
- from Publishers, Advertisers, Subnetworks and payment providers;
- from service providers supporting hosting, analytics, CRM, email, fraud prevention, support, accounting, payments, security and compliance;
- from public sources, business partners, social login providers or platforms where you choose to connect them;
- from authorities or third parties where necessary for legal, fraud prevention or security purposes.

5. Purposes, legal bases and retention

Purpose	Examples	Legal basis under GDPR	Typical retention
Account registration and contract performance	Creating accounts, providing Interface access, Program participation, support, reporting	Art. 6(1)(b) or Art. 6(1)(f)	For the term of cooperation and then for limitation periods
Payments, invoicing and tax	Commission statements, payouts, VAT/tax records, accounting	Art. 6(1)(b), Art. 6(1)(c), Art. 6(1)(f)	Generally 5 years from the end of the relevant tax/accounting year or longer if required
Affiliate tracking and attribution	Click IDs, cookie IDs, postbacks, conversion reporting, commission allocation	Art. 6(1)(f), and consent for device access where required by ePrivacy/PKE/local law	Tracking event data usually up to 24 months, unless needed longer for disputes, fraud, tax or legal claims
Fraud prevention and network quality	Bot detection, duplicate detection, sanctions checks, traffic scoring, investigations	Art. 6(1)(f), Art. 6(1)(c) where applicable	For the period necessary to protect the Network, usually up to limitation periods
Security and service integrity	Login logs, abuse prevention, incident response, backups	Art. 6(1)(f), Art. 6(1)(c)	Security logs usually up to 24 months, longer if needed for incidents
Legal compliance	Responding to authorities, sanctions, tax, accounting, DSA-related notices	Art. 6(1)(c), Art. 6(1)(f)	As required by law or limitation periods
Claims and dispute handling	Complaints, chargebacks,	Art. 6(1)(f)	Until claims expire or proceedings end

	validation disputes, litigation		
Marketing to business contacts	Newsletters, product updates, event invitations	Art. 6(1)(f) or Art. 6(1)(a); electronic marketing consent where required	Until objection, unsubscribe or consent withdrawal
Website analytics and improvement	Analytics cookies, usage statistics, usability	Art. 6(1)(f) or Art. 6(1)(a) depending on technology and local law	According to cookie/tool settings
Recruitment	Candidate assessment and communication	Art. 6(1)(b), Art. 6(1)(c), Art. 6(1)(a), Art. 6(1)(f)	For the recruitment process, then as required by law or consent for future recruitment

We may retain anonymised or aggregated data indefinitely because it no longer identifies an individual.

6. Cookies and similar technologies

Conversand and our partners may use cookies, pixels, tags, local storage, server-to-server postbacks, click IDs, device identifiers and similar technologies for:

- essential website and Interface functionality;
- security and fraud prevention;
- affiliate tracking, attribution and reporting;
- analytics and performance measurement;
- remembering preferences;
- debugging and service improvement.

Where required by law, non-essential cookies and similar technologies may be used only after valid consent. Publishers and Advertisers must collect and document End User consent where their websites, apps or channels trigger Conversand tracking technologies.

You can control cookies through browser settings and, where available, consent management tools. Blocking tracking technologies may affect attribution and commission reporting.

7. Electronic marketing

Where required by law, including the Polish Electronic Communications Law, we send electronic commercial communications only with the required consent or other valid legal basis. You may unsubscribe or object to marketing at any time by using the unsubscribe link or contacting us.

Publishers must not send email, SMS, push notifications, direct messages or other commercial communications promoting Advertiser Programs unless they have all consents and disclosures required by applicable law.

8. Profiling and automated screening

We may use automated tools to support fraud prevention, sanctions screening, traffic quality scoring, security, duplicate detection and Program compliance. These tools may flag accounts, clicks, leads, sales or traffic sources for review and may contribute to payment holds, rejection of Actions, Program suspension or account suspension.

We do not intend to make decisions based solely on automated processing that produce legal effects or similarly significant effects without human involvement where such involvement is required by law. You may contact us if you believe an automated assessment has materially affected you and you want to request review.

9. Sharing personal data

We may share personal data with:

- Advertisers, Publishers and Subnetworks to operate Programs, validate Actions, investigate disputes and pay Commissions;
- payment providers, banks and tax/accounting service providers;
- hosting, cloud, IT, analytics, CRM, email, support, fraud prevention, security and compliance vendors;
- legal, tax, audit and professional advisers;
- affiliates, successors, acquirers or entities involved in corporate transactions;
- courts, regulators, law enforcement, tax authorities and other public bodies where required or justified;
- third parties where necessary to enforce agreements, protect rights, prevent fraud, respond to notices or protect End Users.

We require service providers processing personal data on our behalf to protect data and use it only for agreed purposes.

10. International transfers

Conversand operates internationally. Personal data may be processed in the European Economic Area and in other countries where we, our partners or service providers operate.

Where personal data is transferred outside the EEA, UK or Switzerland to a country without an adequacy decision, we use appropriate safeguards where required, such as Standard Contractual Clauses, UK transfer mechanisms, the EU-U.S. Data Privacy Framework where applicable, transfer impact assessments, contractual protections and security measures.

You may contact us for more information about transfer safeguards.

11. Security

We use technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures may include access controls, encryption in transit, logging, backups, vendor controls, personnel confidentiality and incident response.

No online service can guarantee absolute security. You are responsible for keeping account credentials confidential and notifying us of suspected unauthorised access.

12. Your rights

Subject to legal conditions and limitations, you may have the right to:

- access your personal data;
- rectify inaccurate data;
- erase data;
- restrict processing;
- object to processing based on legitimate interests, including direct marketing;
- receive data portability;
- withdraw consent at any time where processing is based on consent;
- lodge a complaint with a supervisory authority.

The Polish supervisory authority is the President of the Personal Data Protection Office (UODO), <https://uodo.gov.pl>.

To exercise rights, contact mail@conversand.com. We may need to verify your identity before responding. If your request concerns data controlled by a Publisher or Advertiser, we may direct you to that entity or cooperate with it.

Depending on your location, you may have additional rights under local law, such as California/U.S. state privacy laws, UK GDPR, Swiss law, LGPD or other applicable privacy laws.

13. Children and minors

Conversand is intended for business and professional users who are at least 18 years old. We do not knowingly collect personal data from children through account registration. End Users under the age required by local law should not interact with campaigns that are not intended for them.

Publishers and Advertisers must not target minors unlawfully and must comply with special rules for advertising to children, including restrictions on profiling and targeted advertising where applicable.

14. Third-party websites and platforms

Conversand may link to Advertiser websites, Publisher websites, social media platforms, payment providers and other third-party services. Those third parties process personal data under their own privacy notices. We are not responsible for third-party privacy practices unless we act jointly with them under a specific arrangement.

15. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. The current version will be published on our website or in the Interface. Where required or appropriate, we may also notify account users by email or Interface notice.

16. Contact

For privacy questions, rights requests or complaints, contact:

Affluencer sp. z o.o. sp. k.
27 Stycznia 9
34-120 Andrychow
Poland
Email: mail@conversand.com