Crossnetics Inc. Privacy Policy

THIS PRIVACY POLICY IS DEVELOPED DUE TO OUR COMMITMENT TO THE PRINCIPLE OF "ACCOUNTABILITY" IN ACCORDANCE WITH ARTICLE 5(2) OF THE GDPR.

IF YOU HAVE ANY QUESTIONS RELATED TO YOUR RIGHTS, YOU CAN CONTACT OUR **DATA PROTECTION OFFICER (DPO)**

AT **dpo@crossnetics.io** or via the contact form on our website.

BY USING THE CROSSNETICS.IO WEBSITE, YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THE COLLECTION OF COOKIES, THE PURPOSES AND METHODS OF OBTAINING AND PROCESSING PERSONAL DATA, THAT THE DATA YOU PROVIDE IS PROCESSED BY PROFILING, AND YOU GIVE YOUR CONSENT TO THE PROCESSING OF PERSONAL DATA AND ITS TRANSFER TO THIRD PARTIES IN ACCORDANCE WITH THIS POLICY.

ALL DATA YOU PROVIDE IS A PREREQUISITE FOR FULFILLING THE TERMS OF SERVICE FOR USING THE SITE.

The Site and Services, as described in our Terms of Service, are provided to you by Crossnetics Inc., a corporation registered in Delaware, USA, with its registered office at 8 The Green STE A, Dover, DE 19901, USA ("Crossnetics").

Accordingly, "We", "Us" and "Our" refer to Crossnetics Inc.

1. DATA CONTROLLERS AND DATA PROCESSORS

Regarding the processing of personal data of our Services' customers ("Customers") and regarding the Services where we determine the purposes and means of processing personal data of social media users ("Influencers"), **we** are the "Data Controller" for the personal data of Customers and the personal data of Influencers, respectively.

Feel free to send us any of your data protection inquiries at **dpo@crossnetics.io**.

For services (e.g., *Campaign Management*) where the Customer determines the purposes and essential means of processing Influencers' personal data (e.g., *which* and *whose* personal data to process, *how long* to store it), but where we may still determine the technical means of processing personal data (e.g., *where* and *how* to

search, collect, store personal data), and We process personal data on behalf of Customers or on the orders of Customers and in the interests of Customers (*where our Services are to provide a tool to Customers to reach the Customers' purposes*), the **Customer** is the **Controller**, and **we** are the **Processor** (or **Data Processor**).

This Privacy Policy describes how we handle certain personal data of Customers and Influencer data.

We comply with and fully adhere to all regulations concerning personal data, both from European legislation and US legislation, related to personal data (**"Applicable Law"**).

All provisions of this Privacy Policy are drafted in accordance with European personal data compliance legislation (Regulation (EU) 2016/679 General Data Protection Regulation ("GDPR")), and are also aligned with, comply with, and do not contradict the requirements of US personal data protection legislation (in particular, we have used the provisions of the California Consumer Privacy Act (CCPA)).

2. What personal data and data is processed and legal bases for processing

Through this Privacy Policy, we fulfill our obligation under Articles 13 and 14 of the GDPR to provide information about data processing to the relevant data subjects.

DISCLAIMER: However, in some cases (especially when we obtain personal data not from the data subjects, e.g., from social networks) we are unable to inform each data subject (especially influencers) directly, other than through this Privacy Policy. In accordance with Recital 62 and Article 14(5)(b), we are permitted to do this because providing such information proves impossible or would involve a disproportionate effort due to the large number of influencers (in particular for processing for statistical purposes). Nevertheless, we undertake to take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject.

2.1. CUSTOMERS

There are various types of information we collect, whether directly from you during registration (Article 13 GDPR) or automatically through your device (e.g., personal computer, laptop, mobile phone) when you use our Sites (Articles 13-14 GDPR). In accordance with the principle of "data minimization" (Article 5(1)(c) GDPR), we collect and process only what is strictly necessary to provide you with our Services, no more and no less.

Personal data we collect directly from you:	Legal basis for processing (Article 13(1)(c) GDPR)	Purposes for processing (Art. 13(1)(c) GDPR): Reason for collection
1. Full Name	Performance of the contract with you (Art. 6(1)(b) GDPR). We will only retain limited information to respect your opt-out preferences.	You know our name, we require yours for the contractual relationship between the parties.
2. Email Address	1) Performance of the contract with you (Art. 6(1)(b) GDPR) and 2) Our legitimate interests, if related to marketing (Art. 6(1)(f) and Recital 47 GDPR).	1) We require your email to log in and provide you with the Service, reports, service-related updates, messages, and other important information. 2) If we use your email to contact you for marketing purposes, it will be in our legitimate interests, but you will always have the opportunity to opt-out of such marketing messages for similar products and/or services prior to the first (and any subsequent) communication. You can opt out at any time by writing to support@crossnetics.io

Personal data collected/accessed by us automatically

1. **Internet Protocol (IP) Address**
2. *We set and access various cookies on your device**

Legal basis for processing (Article 14(1)(c) GDPR) Performance of contract (Article 6(1)(b) GDPR). You need this to connect to the Internet. Performance of contract for "strictly necessary" cookies. Legitimate interest for first-party analytics cookies (Art. 6(1)(f) GDPR). Your consent prior to the placement of all other types of cookies (Art. 6(1)(a) GDPR).

** This is part of the information that is automatically transmitted from your electronic device when using your browser. More information about what information your browser transmits can be found on the browser companies' websites (e.g., Chrome). You can disable the transmission of cookies at any time in your browser settings.*

2.2. INFLUENCERS

Essentially, we only process information that you have already shared publicly through open social media accounts: Instagram, YouTube, TikTok, Twitch. We process your personal data and guarantee that it will be processed in accordance with applicable law, namely in accordance with the principle of "lawfulness, fairness, transparency" (Article 5(1)(a)), and we respect your rights (see section below).

Influencer Information (categories of personal data):

1. Influencer profile link, full name, avatar, language, biography, country/city/state, brand and general interests, known engaged users, sponsored posts.
2. Email address and social media profile.
3. Images, graphics, photos, profiles, audio and video clips, sounds, musical works, audience connections, comment texts, works of authorship, applications, links and other content or materials from your social media profile.

Legal basis for processing (Article 14(1)(c) GDPR) Influencers provide their data to social networks, thereby making it publicly available. We process data that we obtain from public sources (Instagram, YouTube, TikTok, Twitch). We have a legitimate interest in using the data provided by influencers through social networks for direct marketing purposes (Recital 47 GDPR), without affecting the fundamental rights and freedoms of the Influencer.

Purposes for processing (Art. 14(1)(c) GDPR): Grounds for collection To allow customers to select an influencer for their business purposes and evaluate the effectiveness of each influencer's reach.

2.3. AUDIENCE DATA AND STATISTICS

We analyze vast amounts of information to provide customers with statistics. Regarding the Influencer's audience ("Audience"), this includes, in particular: gender, age group, and ethnicity. While these items may represent a somewhat sensitive issue, we have conducted, in accordance with Article 35(7)(a) GDPR, an assessment to identify and demonstrate our legitimate interests and to rule out that our legitimate interests are overridden by the fundamental rights and freedoms of the audience or any individuals (Article 6(1)(f) GDPR). We concluded that our processing for statistical purposes complies with applicable law and does not contradict the fundamental rights and freedoms of individuals.

To lawfully process data about the audience's ethnic origin, we require an appropriate legal basis. One basis is processing for statistical purposes (Art. 9(2)(j) GDPR) (while safeguarding the fundamental rights and interests of the audience) and the fact that such data (Article 9(2)(e)) has been made manifestly public by the data subject. Such processing does not have a discriminatory impact on individuals and does not lead to such measures being taken. Finally, there is no automated decision-making and profiling based on the audience's ethnic origin (Art. 14(2)(g) GDPR).

3. What we do with your personal data and aggregated data

Our legitimate interests in handling personal data are the purposes of direct marketing, as stated in Recital 47 GDPR (EU GDPR), and statistical purposes refer to Recitals 113 and 162 GDPR.

However, under US law (e.g., the California Consumer Privacy Act), there is no concept of legitimate interest. The law does not list specific grounds for processing, although the sale of consumer information is prohibited if the consumer has opted out. Therefore, we clearly offer each of our INFLUENCERS the use of the opt-out function.

3.1. CUSTOMERS

We do not sell, share, or disclose Customer data, except as provided herein. We never treat your personal data in any way that would surprise you (unless we have told you about it and you have provided us with informed and unambiguous consent for such use).

We use Customer contact data and payment information to establish, support, and conduct customer relationships as necessary to perform the Services. If a Customer does not provide the personal data we need, we will not be able to complete the transaction. We contact Customers only with service-related information. In cases where marketing is involved, customers have the opportunity to opt out at any time prior to the first (and any subsequent) contact.

3.2. INFLUENCERS

Notification of the processing of Influencer personal data occurs through our website and through the provisions of this Policy. Due to the processing of vast amounts of data, we do not have the technical ability to notify each influencer directly. Also, in accordance with the Terms of Service and Agreements with Customers, the obligation to notify the Influencer about the processing of his/her personal data is transferred to the Customer.

We provide statistical services, and therefore the Influencer data listed above is transferred to customers either on a trial basis or upon payment of fees.

The data about Influencers that we process is divided into two categories:

- **Raw Data** - All available information collected from social networks. Information is collected only from public / open profiles of Influencers on Instagram, YouTube, TikTok, Twitch. Raw data is not structured, so the Influencer identity cannot be determined based on this information. Processed Data is formed from Raw Data, and then Reports are generated.
- **Processed Data** - is formed from Raw Data. The Processed Data is divided into two groups:
    - Collected and stored as is: profile name, avatar, profile description, likes, commenters, email;
    - Data generated by AI scripts: audience type, topics and interests of the audience, age of the audience, earnings, history of profile development, authenticity of the audience set.

At any stage of data collection, Influencers have the right to send a request to our Data Protection Officer at **dpo@crossnetics.io** for the purpose of changing / deleting their data.

3.3. AUDIENCE DATA

Audience data for each Influencer is aggregated for statistical purposes and shared with Customers whether on a trial basis or upon payment of fees.

3.4. DATA CONTROLLER

The Data Controller can use the collected data itself as a marketing advertiser. Such Data Controller's report will be identical to a regular Report provided to any Customer. Such Reports are subject to laws and regulations applicable to all Data Controller's activities.

4. Where and how long personal data is stored for

In compliance with Article 5(1)(b), (c), (e) GDPR, We commit to the principles of "purpose limitation", "data minimization", "storage limitation", and therefore We collect, retain, store and otherwise process only such information that is necessary to ensure our legitimate interests or to comply with a legal obligation, and for the period necessary to meet our legitimate interests.

4.1. CUSTOMERS

We store your data while your account is active. Whether your annual subscription expires or you fail to use the credits on time, We will delete your personal data from our systems within 1 (one) month after expiration of your annual subscription or when you request such deletion in the frame of exercising your rights (as listed below).

4.2. INFLUENCERS

As stated above, We process the personal data obtained from public sources (open accounts on Instagram, YouTube, TikTok, Twitch). The updates may take up to 20 days.

If an Influencer deletes his/her account, We will also delete such personal data from our systems and make it unavailable to Customers. This synchronization may take up to 1 (one) month from the date the Influencer deleted his/her account on the relevant social networks.

4.3. AUDIENCE DATA

Audience data is only relevant to the Influencer and is kept in aggregated form together with information about the Influencer. Once Influencer data is deleted, the Audience data of the Influencer is also deleted.

5. Security measures used by Us

In compliance with Article 5(1)(d), (e), (f) GDPR, We commit to the principles of "accuracy", "storage limitation", and "integrity and confidentiality".

All personal data is stored by our third-party (sub-)processors on secure servers (AWS Amazon, Digital Ocean and Hetzner) **located in the Netherlands**, in full compliance with international information security requirements. AWS Amazon and Digital Ocean possess ISO 27001 information security management system certificates. We use recommended industry practices to secure access to such data (a mix of common sense and best practices). All data is stored in encoded form. It is impossible to obtain the personal data of any influencer without their specified storage identification code.

We use appropriate levels of technical and organizational measures to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. Those include the following:

(1) **Protective measures for physical access control:** We secure access to the premises via ID readers, so that only authorized persons have access. The ID cards can be blocked individually; access is also logged. Furthermore, an alarm system is installed on the premises to prevent unauthorized entry. The alarm system is linked to a door locking mechanism.

(2) **Protective measures for system access control:** Each employee has access to the systems/services only via his/her own employee access. The access rights involved are limited to the responsibilities of the respective employee and/or team. We regulate access to our own systems via password procedures and the use of SSH keys of at least 1024 bits in length. The SSH keys strengthen the productive systems against attacks that target weak passwords, as the password-based access to the relevant systems is disabled. We also have a password creation policy. This ensures higher security also for systems that offer password-based access. Passwords must meet the following requirements: at least 8 characters long, one capital letter, one digit, one specific

character. Our systems are protected by firewalls that reject all incoming connections by default. Only connection types defined by exception are accepted.

(3) **Protective measures for data access control:** All servers and services are subject to continuous monitoring. This includes the logging of personal access in the user interface. Due to the close proximity of the employees, a visual inspection is possible at any time. Locking and/or logging off when leaving work is prescribed in writing and is practiced.

(4) **Protective measures for transfer control:** The handling of local data storage devices, e.g. USB sticks, is regulated via agreements. Access to the systems from outside the company network is possible only via secure VPN access.

(5) **Protective measures for input control:** Our employees do not work directly at the database level, but instead use applications to access the data. IT employees access the system via individual access and use a common login, as there are very few employees and these sit in close proximity to each other and monitor each other by agreements and visual inspections.

(6) **Protective measures for availability control:** We ensure availability of data in several ways. On the one hand, there is regular backup of the entire system. This steps in if the other availability measures fail. Critical services are operated redundantly in multiple data centers and controlled by a high-availability system. Our workstations are also protected with the usual measures. For example, virus scanners are installed, laptops are encrypted. We ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (Art. 32(1)(c) GDPR). We automatically produce back-up copies of all the data, and in case of data loss, we are able to restore such data from those back-ups.

(7) **Protective measures for separation control:** To separate data, We use logically separate databases so that no accidental reading of data by unauthorized persons can occur. Access to the data itself is also restricted by the fact that employees use services (applications) which control access.

(8) **Measures in case of personal data breach.** Our IT devices are equipped with passwords and encryption by default. In case of loss/theft of a device, our impacted employee follows his/her duty of internal notification and We block all access, deactivate keys and change passwords. In the event of a data breach (e.g., a leak), we undertake to investigate the matter, promptly notify the competent data protection authority, assess the damage, and report the investigation results to all customers whose personal data has been affected.

We take our responsibility seriously and have therefore implemented various technical and organizational measures ("TOMs") to protect and safeguard personal data as best

as possible. Our measures are consistent with the rules of the GDPR (Articles 24, 25 and 32).

6. Categories of recipients of personal data and data

We do not rent, sell, or share Customer personal data with any third parties, except where We have to comply with Our legal obligation.

We provide a paid statistical service regarding Influencer and Audience data. The recipients of such data are Customers of our Service.

Regarding Customer data, We do not blindly comply with disclosure orders. We will review each request to ensure that it satisfies the relevant safeguards, contains a court order, or is issued under a legislative measure to prevent, investigate, detect or prosecute criminal offenses.

If we hire a (sub-)processor to act on our behalf, we guarantee that there are adequate contractual measures in place to ensure responsibility, security, and accountability at the same level as from us. All Data (both Raw Data and Processed Data) that we collect is stored in a database controlled and maintained by our sub-processors.

In any case where a third party accesses your data on our behalf or according to Our instructions (inside or outside the EEA), we use the appropriate legal basis to comply with data protection legislation. In those cases where there is no European Commission decision confirming an adequate level of protection (Art. 45(1) GDPR), We use the standard data protection clauses adopted by the European Commission (Art. 46(2)(c) GDPR), to ensure appropriate safeguards for your rights and personal data in the event of third-party access or other data transfer outside the EEA.

7. Your rights

In accordance with Article 5(1)(a), (d) GDPR, we commit to the principles of "lawfulness, fairness and transparency" and "accuracy".

7.1. You are entitled to the full spectrum of the rights under the General Data Protection Regulation, and We commit to respect your rights. Among those, you have the right to:

- Require access to your personal data (Art. 15 GDPR);
- Require correction of your personal data (Art. 16 GDPR);
- Require deletion of your personal data (Art. 17 GDPR);
- Require restriction of processing of your personal data (Art. 18 GDPR);
- Require portability of your personal data (Art. 20 GDPR);
- Object to the processing of your personal data (Art. 21 GDPR);
- Object to automated processing (if any) of your personal data (Art. 22 GDPR);
- Withdraw your consent to the processing of your personal data, where applicable (Art. 7(3) GDPR);

- Lodge a complaint with your national supervisory authority (in the EEA), if you believe your privacy rights have been violated (Art. 13(2)(d), 14(2)(e), 15(1)(f)).

7.2. Your consent and your right to withdraw your consent

If we decide to process your personal data for any purposes you disagree with, we will provide you with relevant information at the time you encounter these additional purposes to obtain your consent (if required) or to be able to fulfill Our legal obligations, prior to commencing any such additional processing. You are not obliged to give consent just because we ask for it.

If your personal data has been processed on the basis of your consent, you may change your mind and withdraw your consent later by contacting our Data Protection Officer ("DPO") and requesting removal from the mailing list at the following email address **dpo@crossnetics.io**. However, your withdrawal of consent will not affect the processing of your personal data that occurred before your withdrawal.

7.3. Your right to object to data processing

If your personal data has been processed without your consent (on the basis of legitimate interests), you can also ask us to stop processing your personal data and remove you from the mailing list by contacting our DPO at **dpo@crossnetics.io**. However, your request will not affect the processing of your personal data that took place prior to such request.

If you ask Us to correct, delete your personal data or restrict the processing of your data (to stop processing or by withdrawing your consent), we will inform you as soon as your request is satisfied (in accordance with Art. 13(2)(c), 14(d) and 19 GDPR).

7.4. Your right to lodge a complaint

If your issue is not resolved or resolved satisfactorily, you have the right to contact your local data protection authority (Art. 13(2)(d), 14(2)(e), 15(1)(f)). You can find the contact details of your local data protection authority here: **https://edpb.europa.eu/about-edpb/board/members_en**

7.5. INFLUENCERS: your right to be informed about the Customer

You have the right to request information about the Customer who received the personal data of your social media profile, and Crossnetics undertakes to provide you with all information about the Customer.

If you request information about the Customer who received your personal data, Crossnetics will provide you with all information about the Customer within 72 hours of receiving your request.

If the Customer has transferred to third parties a Report on your social media profile obtained using the Crossnetics service, you have the right to receive the entire chain of persons to whom such Report was transferred within 72 hours of your request.

7.6. Your right to access and delete your personal data

You have the right to request the deletion of data/content collected from our Service. Such data/content must be deleted within 72 hours of notification. Furthermore, the data/content must be deleted by all persons/companies/reviewers to whom such information was transferred.

You have the right to log into your account and change information about yourself to the extent permitted by the system. You can also submit a request to change your information to support.

8. Cookies and similar technologies

We use aggregated, non-identifying electronic data collected using our Sites and Services to operate, analyze, improve, and develop our Sites and Services. This information is not used to inform decisions about specific individuals; rather, it is processed to understand how different categories of users interact with our sites and services so that we can consistently improve the same for customers.

We work with analytics providers such as Google Analytics, which use cookies and similar technologies to collect and analyze information about the use of the Services and report on activities and trends. Google Analytics may also collect information about the use of other websites, applications and online resources. You can learn about Google's practices by going to www.google.com/policies/privacy/partners/, and opt out of them by downloading the Google Analytics browser add-on.

We inform you that in order to satisfy our legitimate interests and improve the quality of services, we may transfer some personal data that is publicly available on social networks to the following service providers:

- Amazon Web Services, Inc.
- Digital Ocean, LLC
- Hetzner Online GmbH
- PayPal, Inc.
- Stripe, Inc.
- Amplitude, Inc.
- HubSpot, Inc.
- Intercom, Inc.
- Google Inc.
- FullStory, Inc.

Some user data collected by us may be collected from third parties using custom integrations, using third-party policies that limit the permitted purposes for which this data can be used. For example, when working with data obtained through Google APIs,

the Service uses user data only in accordance with the Google API Services User Data Policy.

We also inform you that Crossnetics' use and transfer of information received from Google APIs to any other app will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

You can get more detailed information about those service providers and the type of data they process at this link: [Provide link to an up-to-date list of processors on Google Sheets or another resource]

The service providers Hubspot, Amplitude, Google Analytics and Intercom are located in the USA. We have entered into contracts with them by purchasing their software and maintenance services (which will be used for marketing and customer communication) and by accepting their customer terms and privacy policies published on their websites:

- Amplitude: https://amplitude.com/privacy
- HubSpot: https://legal.hubspot.com/privacy-policy
- Google: https://policies.google.com/privacy?hl=en-US
- Intercom: https://www.intercom.com/legal/privacy

Regarding the transfer (import/export) and processing of personal data subject to the GDPR, Hubspot, Google and Intercom rely on the EU Standard Contractual Clauses; and Amplitude relies on compliance mechanisms recognized by the GDPR (the EU-US Privacy Shield was invalidated, so alternatives such as Standard Contractual Clauses should be indicated).

9. Children's privacy (Article 8 GDPR)

We never knowingly collect, process or request any information from anyone aged 16 and under. Information society services ("Services") on our sites are not offered directly and are not intended to address such individuals. Parents or holders of parental responsibility who believe that we directly offer Services or process the personal data of their children under the age of 16 can contact Our DPO at **dpo@crossnetics.io**.

DISCLAIMER: When processing open data from social networks, if it is reasonably impossible to recognize the actual age of users, Our verification of user age is limited to technically available and reasonable processing of information openly provided by the social networks from which we collect data. In case of erroneous, incorrect or missing age data, the social networks bear sole responsibility for violating the requirements of Applicable Law regarding children's personal data.

10. Our commitment

- We will collect and use your data only where we have a legal basis for doing so;

- We will always be transparent and tell you about how we use your information;
- When we collect your data for a specific purpose, we will not use it for anything else without your consent, unless another legal basis applies;
- We will not ask for more data than is necessary to provide our services;
- We will adhere to a data retention policy and ensure that your information is securely disposed of at the end of such retention period;
- We will comply with and respect Your Rights, ensuring prompt and transparent handling of matters concerning privacy issues;
- We will support our employees in their duties of confidentiality and security;
- We will ensure that appropriate technological and organizational measures are taken to protect your data wherever it is stored;
- We will also ensure that all our data processors (sub-) have appropriate security measures with contractual provisions requiring them to comply with our obligations;

11. Changes to the privacy policy

To keep you informed, we will always notify you by email if we update this privacy policy.

Crossnetics Inc.,
8 The Green STE A,
Dover, DE 19901, USA

Effective Date: January 01, 2025